UNIVERSIDAD DE SOTAVENTO

INCORPORADA A LA UNAM

LICENCIATURA EN INFORMÁTICA

"SEGURIDAD EN EL COMERCIO ELECTRÓNICO"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN INFORMÁTICA

P R E S E N T A

MARGARITA MADRIGAL CRUZ

ASESOR:

L.I. EMILIO DE JESÚS ESPRONCEDA GONZÁLEZ

Coatzacoalcos, Ver *Septiembre 2013*

DEDICATIORIAS

A Dios Todo poderoso, por guiar cada paso que he dado en mi vida, ya que ha sido con la certeza de que estás a mi lado llenando mi corazón con la luz de tu espíritu y es por ello que he alcanzado cada meta propuesta. Por ser quien me brindo la dicha de vivir y de regalarme una familia maravillosa, que ha estado a mi lado en todo momento.

Dedico este proyecto, a mis padres Yolanda Cruz y Guillermo Madrigal, por todo el apoyo que me han brindado durante mi trayecto, por ese cariño, amor y confianza que me brindaron, y que gracias a ellos soy quien soy hoy. Porque ustedes son los que han velado por mi salud, mis estudios, mi educación, son a ellos a quien les debo todo, horas de consejos, de regaños, de reprimenda, de tristezas y de alegrías de las cuales estoy muy segura que las han hecho con todo el amor del mundo para formarme como un ser integral y de las cuales me siento extremadamente orgullosa.

A mis hermanos por estar conmigo y apoyarme siempre.

Y a todas las personas que han estado presentes en mi vida y que me han brindaron de su apoyo y cada uno de sus consejos. Por estar siempre conmigo.

¡Familia Los Amo!

Para empezar un gran proyecto, hace falta valentía.

Para terminar un gran proyecto, hace falta perseverancia.

AGRADECIMIENTOS

A Dios.
Agradezco a Dios por darme la vida, por haberme permitido poder llegar hasta este punto y haberme dado salud, sabiduría, inteligencia y las energías para lograr mis objetivos y alcanzar este triunfo, además de su infinita bondad y amor y sobre todo por haberme permitido existir.

A ti Madre.
Por haberme educado y soportar mis errores. Gracias a tus consejos, por el amor que siempre me has brindado, por cultivar e inculcar ese sabio don de la responsabilidad. Y me siento orgullosa de que seas mi madre.
¡Gracias por darme la vida, Te Amo!

A ti Padre.
A quien le debo todo en la vida, le agradezco el cariño, el amor, la comprensión, por creer en mí, la paciencia y el apoyo que me brindó para culminar mi carrera profesional. ¡Te Quiero mucho y Te Amo!

A mis hermanos.
Por brindarme todo su apoyo, cariño y comprensión. Y por cada uno de sus consejos y sus palabras de motivación.

***A Jorge Rivas**.*
Gracias, por todo tu apoyo, comprensión y paciencia, que me brindaste durante todo este tiempo. Por motivarme a seguir adelante. Mil gracias.

A mi asesor L.I. Emilio de Jesús Espronceda González.
Gracias por todo el apoyo y consejos brindados durante este tiempo. Por su tiempo. Deseo que Dios lo bendiga siempre.

A mi asesor M.C.E. Mario Enrique García Maldonado.

Infinitamente Gracias Profesor! Porque sin su ayuda no habría podido culminar esta investigación, gracias por todos sus consejos, gracias por soportarme y por todo su apoyo, tiempo y paciencia que puso en mi. Es un excelente profesor y ser humano, lo admiro por su forma de ser y de pensar. Que Dios lo bendiga siempre y a cada instante de si vida.

Agradezco a todos aquellos que me motivaron, para poder llegar al final de esta investigación. Que confiaron en mí para poder lograrlo Mil palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en todo momento.

ÍNDICE

"SEGURIDAD EN EL COMERCIO ELECTRONICO"

INTRODUCCION

¡Imagínate comprar diferentes artículos! ¡Ahora con un clic puedes tenerlos!

Hoy en día comprar ciertos artículos o transacciones bancarias, ya no es una práctica prohibitiva. Esto es una realidad y todo gracias a las nuevas empresas de venta en línea. Este nuevo modelo de negocio se basa en la compra o venta de artículos a través de portales web.

En la actualidad es una de las principales herramientas para lograr que los negocios pequeños extiendan sus fronteras y posibilidades de compra-venta de productos y servicios, así como también optimizar costos. Cada vez son más los usuarios que realizan compras por internet y esto es debido a que se han ampliado los sistemas de seguridad, los procesos de seguimiento de órdenes, los métodos de pago, la difusión de artículos. Contexto que tratamos en la presente investigación, así como los mecanismos de seguridad que se manejan.

La unión entre los medios de comunicación y la información, conocida como la telemática, ha generado un cambio sin precedentes en el ámbito comercial. El comercio electrónico es el ejemplo más sobresaliente de esta relación, presentando un instrumento de comunicación tan significativo, como la televisión, la radio fusión sonara, la telefonía fija, el celular móvil, el telefax, redes sociales. Por suerte, la misma tecnología que forzó este cambio de paradigma en el comercio continúa evolucionando. Sin embargo, este servicio afronta un gran inconveniente, la inseguridad, razón por la cual se proporciona al usuario una visión técnica y teórica sobre los aspectos más relevantes del comercio electrónico y su seguridad.

Garantizar la seguridad es quizá el más importante tema para las personas interesadas en efectuar operaciones dentro de un sitio web. El intercambio de información al momento de realizarse una operación electrónica por medio de redes abiertas genera un riesgo operacional en la medida en que dicha información puede viajar sin ningún tipo de protección. Sin embargo; muchos usuarios nos preguntamos ¿Motivos por el cual no comprar por internet? Muchas de las razones o miedo para no hacerlos, nos encontramos destacadamente con varias razones

relacionadas con la desconfianza al (Anexo1. Gráfica A. Pág. 121) no me da confianza dar mi datos personales, no sé cómo comprar por internet, no tengo tarjeta de crédito, me da miedo proporcionar datos de mi tarjeta de crédito.

La situación actual de desarrollo, computacional y de redes de información, ha puesto de manifiesto la importancia de detectar, prevenir y detener las violaciones a la seguridad en la red.

Hoy en día y por medio de la presente investigación, se puede afirmar que existen mecanismos y herramientas para garantizar un alto nivel de seguridad en la red. Existen aseguradoras que ofrecen seguros de responsabilidad civil, de robos, existen los firewalls, equivalentes a los guardas de seguridad en la red los cuales permiten el acceso a ciertos usuarios y deniegan a otros, también existen los certificados digitales, sellos de confianza, autenticas llaves de seguridad de la puertas virtuales de la tienda electrónica que a la vez permiten garantizar el no repudio de las transacciones, entre otros mas, que son temas de abordar en la investigación.

Por medio de la presente investigación los usuarios podrán conocer los mecanismos que se utilizan para la seguridad en la red, los tipos de herramientas entre otros temas. Los temas abordados serán de interés, para que puedan comprender de mejor manera como es el comercio electrónico y de qué forma pueden detectar cuando se encuentran dentro de un sitio web seguro.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente el internet ha adquirido durante los últimos años una gran importancia para la sociedad. Podemos decir que se encuentra dentro de un ámbito que involucra un sinfín de aspectos importantes, se ha convertido en un medio que tiene presencia en múltiples aspectos dentro de la sociedad mediante correos electrónicos y blogs, hasta compras de bienes y servicios y trámites gubernamentales, entre otros usos. Está cada vez más presente en nuestras actividades diarias. El desarrollo de estas tecnologías, ha hecho que los intercambios de datos crezcan a niveles extraordinarios, simplificándose cada vez más y creando nuevas formas de comercio, y en este marco se desarrolla el Comercio Electrónico.

Que hoy en día la seguridad en el comercio electrónico ha adquirido gran auge, este ha iniciado una revolución tanto o más grande que lo industrial y no podemos sustraernos de los cambios que ha originado, sobre todo en la forma de hacer negocios, y como saber si lo que estamos haciendo se realiza de forma segura, dadas las cambiantes, condiciones y nuevas plataformas de computación disponibles, situación que desembocan la aparición de nuevas amenazas en los sistemas informáticos. La seguridad, en este ambiente involucra las siguientes partes: **Privacidad, Integridad, No Repudio**, **Autenticación** y **Facilidad**.

La mayoría de los usuarios no confía en las páginas de internet como canal de pago, pues este no dispone de información del entorno que gira alrededor de la seguridad en el comercio electrónico. En la actualidad, las compras se realizan utilizando el número de la tarjeta de crédito, pero aún no es seguro introducirlo en Internet sin conocimiento alguno. Cualquiera que transfiera datos de una tarjeta de crédito mediante alguna página de internet, no puede estar seguro de la identidad del vendedor. También existen de forma alarmante los fraudes electrónicos, especialmente el robo de identidad. Esta nueva modalidad de fraude, comúnmente se refiere a toda aquella información de un individuo, que es obtenida y utilizada sin su consentimiento, y con el propósito de cometer actividades fraudulentas.

Podemos decir que esto también pasa por que no hay una seguridad a la hora de ingresar datos personales, cuando se va a realizar cierta compra en alguna página de internet.

1.2 OBJETIVOS

Existen diferentes formas de hacer comercio electrónico, y su clasificación aún está por formarse, sin embargo, la parte más visible es la que cualquier usuario en una computadora personal puede hacer, que esto se convierta en comprar o vender usando una conexión de Internet en lugar de ir a la tienda real. Al efectuar una operación comercial por la WEB se presentan nuevos problemas, por ejemplo, cómo saber que la tienda virtual existe verdaderamente, una vez hecho el pedido cómo saber que no se cambia la información, cuando se envía el número de tarjeta de crédito y cómo saber si este permanecerá privado, en fin. Por este motivo, el objetivo consiste en analizar y describir como el usuario puede identificar cuando se encuentra dentro de un sitio WEB seguro. Y si el sitio donde se encuentran cuenta con seguridad para poder introducir datos importantes o realizar ciertas transacciones. Mostrar cuales son las tecnologías de protección con las que se cuentan actualmente y un análisis detallado de las herramientas de apoyo para la seguridad de las aplicaciones WEB.

1.2.1 OBJETIVO GENERAL

Analizar y describir la seguridad en el comercio electrónico. Para que el usuario pueda identificar cuando se encuentra dentro de un sitio WEB seguro. Presentando cada uno de los mecanismos de seguridad.

1.2.2 OBJETIVOS ESPECÍFICOS

- Identificar cuando el usuario se encuentra dentro de sitio seguro.
- Presentar los elementos involucrados dentro de la seguridad del comercio electrónico.
- Establecer los pasos necesarios para la implementación de un sitio WEB seguro.

1.3 PREGUNTA DE INVESTIGACION

¿Cómo identificar que existe seguridad, en un sitio de comercio electrónico?

PREGUNTAS SECUNDARIAS

¿Qué conceptos involucra la seguridad en el comercio electrónico?

¿Cómo identificar cuando un sitio cuenta con seguridad o sellos de confianza para realizar cierta transacción?

¿Cuáles son los pasos necesarios para la implementación de un sitio seguro?

¿Es seguro el comercio electrónico?

¿Cómo un sitio en la web, le transmite confianza al cliente para realizar transacciones?

¿Cuándo se debe aplicar la seguridad en el tipo de transacciones, en envió de información, los pagos interbancarios con tarjetas de crédito u otros aspectos?

1.4 JUSTIFICACIÓN

El internet se ha convertido en un mercado global para bienes y servicios. Para que este mercado prospere, los compradores deben de sentir confianza en el momento en el que transmiten los números de su tarjeta de crédito, datos personales o cualquier otra información financiera. Debido a que los datos que se envían pasan por muchas computadoras en su recorrido hacia su destino final, existe la posibilidad de que alguien intercepte información confidencial.

Por ello, el propósito es analizar los aspectos generales del comercio electrónico, las diferentes tecnologías y la seguridad de la información

Asimismo también se tomara en cuenta, el funcionamiento de la firma digital, robo y falsificación de certificados digitales y los protocolos de seguridad.

La aparición del comercio electrónico obliga claramente a replantearse muchas de las cuestiones del comercio tradicional, surgiendo nuevos problemas, e incluso agudizando algunos de los ya existentes. En ese catálogo de problemas, se plantean cuestiones que van, desde la validez legal y el control de las transacciones, la protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y robo de datos personales, el envió de información importante, la falta de seguridad de las transacciones y medios de pago electrónicos y protocolos de comercio electrónico incompatibles y la congestión de Internet.

1.5 HIPÓTESIS

Si se analizan y describen los pasos para la implementación de la seguridad en el comercio electrónico, aumentará la facilidad y la integridad de los usuarios, para utilizar este medio del comercio.

VARIABLES

Variable independiente: analizar y describir, la seguridad.

Variable dependiente: Facilidad e integridad de los usuarios.

1.6 DELIMITACIÓN DE LA INVESTIGACIÓN.

En este apartado se establecerá descriptivamente la cobertura que tuvo la investigación en lo relativo a:

- Espacio geográfico, el lugar donde se realizará la investigación.
  - ❖ La ciudad de Coatzacoalcos y Las Choapas.

- Sujetos y/u objetos que participaron en la realización del estudio.
  - ❖ Encuestas
  - ❖ La sociedad de Coatzacoalcos y de Las choapas
  - ❖ Internet
  - ❖ El comercio electrónico

- Tiempo, en el que será realizada la investigación.

  - ❖ La investigación será realizada en un lapso de 10 meses.

- Contenidos, la o las variables que se consideraron en el estudio.
  - ❖ Seguridad
  - ❖ Comercio electrónico
  - ❖ Internet
  - ❖ Sociedad

1.7 LIMITACIONES

El trabajo realizado en la presente investigación, no esta exento de ciertas limitaciones.

Otro obstáculo con el que se podría contar, es que la personas adultas no accedan a responder las encuestas que se van a realizar, para tener una muestra de las personas que desconocen cómo es la seguridad en el comercio electrónico.

Este tipo de investigación será de tipo exploratoria y explicativa, para poder mostrarles a los usuarios como es la seguridad en el comercio electrónico y cuáles son las implementaciones que se utilizan.

CAPíTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES DEL COMERCIO ELECTRÓNICO

2.1.1 HISTORIA Y EVOLUCIÓN

El comercio electrónico[1], también conocido como e-commerce (electronic commerce en inglés) *definido como el proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación. Representa una gran variedad de posibilidades para adquirir bienes o servicios ofrecidos por proveedores en diversas partes del mundo*

Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el intercambio electrónico de datos, sin embargo con el advenimiento del Internet y la World Wide Web (red de alcance mundial o Red de Amplitud Mundial). Internet se ha consolidado como la plataforma ideal para el desarrollo de pequeñas y grandes empresas, al permitir la globalización de productos y servicios. Es la forma propia de Internet en el que se realiza la transacción económica, compra o venta, de forma ágil, rápida y directa, favorecida por la comodidad y facilidad de utilización por parte de los usuarios. El Comercio Electrónico, el dinero electrónico, el monedero electrónico, son conceptos y términos que ya empiezan a ser reconocidos cotidianamente, y que poco a poco se irán intercalando en el uso y costumbres sociales y económicas.

Hasta hace relativamente poco tiempo, el término COMERCIO ELECTRONICO estaba vinculado estrictamente al alcance del EDI (Electronic Data Interchange), que fue el proceso fuertemente orientado a la transmisión de datos comerciales seguros vía computador (órdenes de compra, transferencias bancarias, etc.) Por sus características y costos estaba prácticamente reservado, sólo podían acceder a su uso el sector financiero y las grandes empresas. El desarrollo de Internet y en especial de la WWW importó una democratización del concepto y sus alcances, permitiendo implementaciones con diversos grados de complejidad y costo,

[1] De Águila Rosa Ana. Comercio electrónico y estrategia empresarial. Pág. 61

abriendo este camino para todo tipo de proyectos. El comercio electrónico también se ha visto beneficiado con estos avances.

A principio de los años 1970, aparecieron las primeras relaciones comerciales que utilizaban una computadora para transmitir datos, tales como órdenes de compra y facturas. Este tipo de intercambio de información, si bien no estandarizado, trajo aparejado mejoras de los procesos de fabricación en el ámbito privado, entre empresas de un mismo sector.

A mediados de 1980, con la ayuda de la televisión, surgió una nueva forma de venta por catálogo, también llamada venta directa. De esta manera, los productos son mostrados con mayor realismo, y con la dinámica de que pueden ser exhibidos resaltando sus características. La venta directa es concretada mediante un teléfono y usualmente con pagos de tarjetas de crédito. 1994, se conectan a internet, servicios como AOL (American OnLine) y Compuserve. Internet se hace accesible para un gran número de usuarios acostumbrados a pagar por navegar.

En 1995 los países integrantes del G7/G8 crearon la iniciativa de un Mercado Global para PYMES, con el propósito de acelerar el uso del comercio electrónico entre las empresas de todo el mundo durante el cual se creó el portal pionero en idioma español Comercio Electrónico Global.

A finales de 1990 y principios de 2000, el comercio electrónico comenzó a ser definido como el proceso de compra de bienes y servicios a través de Internet utilizando los servicios de pago seguros y finaliza la compra electrónica, más parecido a lo que conocemos hoy en día

Las últimas cifras referentes al uso del comercio electrónico reflejan una mejora sustancial, sin embargo no es suficiente. De él se desprende que el comercio electrónico en nuestro país sigue creciendo, y de una forma afortunadamente importante. Los indicadores demuestran que el volumen de ventas en el comercio en línea de 2010 alcanzo cifra record de 36 mil 500 millones de pesos, lo que representa un incremento del 49%.

El comercio electrónico en nuestro país represento en 2011 54, 500 millones de pesos; es decir 4,100 millones de dólares. Se estima un crecimiento del 46% para el cierre de 2013, lo cual representa 79,600 millones de pesos. El 46% de internautas evaluados ha comprado algún producto y/o servicio por internet en sitios nacionales y extranjeros, lo cual representa un crecimiento del 18% respecto al 2012 y una clara búsqueda de opciones diferentes por parte de los internautas en México.

Algunos de los principales retos dentro del comercio electrónico en México es la falta de información, facilitar los procesos de compras, diversificar los métodos de pago y generar confianza al consumidor.

El comercio electrónico es una fuerza dinámica dentro de la economía en México y de todo el mundo entero. El uso del internet en la actividad comercial está revolucionando la forma en la que el mundo corporativo realiza negocio, además está aumentando el poder de la economía, ya que este medio logra comunicar a las grandes empresas con los nuevo lideres comerciales. Las pequeñas empresas tienen acceso a los clientes mediante el uso de internet. Hoy en día, millones de clientes en todo el mundo pueden solicitar bienes y servicios durante las 24 horas del día, los siete días de la semana.

Sin embargo la situación actual del comercio electrónico ha registrado un fuerte crecimiento a escala mundial, tanto en volumen de usuarios como volumen de sitios comerciales y sin duda alguna la inversión publicitaria en la red, por su volumen actual se puede considerar ya un medio de comunicación de masas. Sin duda alguna el comercio electrónico a evolucionado de una manera exponencial y hoy en día es una manera de hacer negocio en la red sin necesidad de realizar grandes inversiones y poder hacerlo directamente de tu casa u oficina siempre y cuando se cuente con una conexión a internet.

2.1.2 GENERACIONES DEL COMERCIO ELECTRÓNICO

Respecto al comercio electrónico, se suelen considerar cuatro generaciones que parten del EDI, o intercambio electrónico de datos (por sus siglas en ingles), servicio que las empresas ya empleaban, al margen de internet.

En generaciones del comercio electrónico:

- **Primera generación[2]:**

Cuando la web empieza a salir de los centros de investigación, allá por el año de 1993, las primeras grandes empresas perciben la importancia y empiezan a crear páginas web sólo hablando de la organización. Posteriormente, aparecen los primeros catálogos en la red. Las páginas son estáticas y, el modo de comunicación con el comprador se reduce a los formularios o correo electrónico.

- **Segunda generación[3]:**

Inmediatamente, las empresas ven la posibilidad de emplear sus páginas para hacer negoció directamente en la red. En esta etapa ya se puede comprar a través de la página. Aparecen los "centros comerciales virtuales" en los que una empresa que disponía de la tecnología e infraestructura necesaria para crear tiendas virtuales, alquilaba espacio a otras empresas interesadas en tener su propia tienda.

En cuanto a los medios de pagos, en esta etapa se suele emplear el pago contra reembolso, cheques, transferencias y, en algunos casos, pago mediante tarjeta electrónica. Empiezan los negocios de internet "puros", empresas que nacen exclusivamente para vender productos o servicios a través de la red.

- **Tercera generación[4]:**

Pretende automatizar el proceso de selección y envío de los datos acerca de los productos comprados. La solución es implementar sistemas de bases de datos junto con aplicaciones web, basadas en guiones CGI (Common Gateway Interface). Aparecen los primeros contenidos dinámicos y se generaliza el "marketing en la red". En cuanto a los medios de pagos, se generaliza el empleo de las tarjeras medio de pago. Aparecen los primeros protocolos para pago seguro.

---

[2] Seoane Balado Eloy. La nueva era de comercio: el comercio electrónico. Pág. 10
[3] Seoane Balado Eloy. La nueva era de comercio: el comercio electrónico. Pág. 11
[4] Ibídem. Pág. 13

- **Cuarta generación[5]:**

El contenido es dinámico, generado mediante una aplicación web a partir de datos suministrados por un sistema de bases de datos. Se cuida el diseño del sitio, empleándose diseñadores gráficos especializados para su creación e informáticos para el soporte y diseño de la lógica del negocio. Se mejora la seguridad de los sitios y se implantan diversos mecanismos de pago seguro.

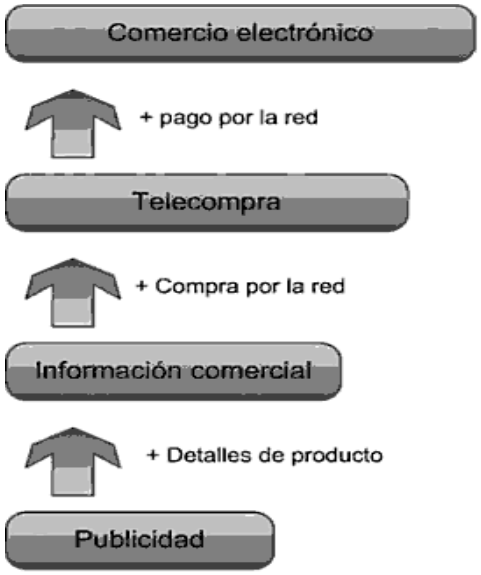


Figura 1.1 Comercio electrónico

[5] De Núñez Alberto Fernando, Lugones. Modelos de negocios en internet. pág.46

2.2 CATEGORIAS DEL COMERCIO ELECTRONICO

Internet ha creado nuevos modelos o categorías de negocios y está obligando a los sectores tradicionales a cambiar de estrategia. Una de las novedades que ha traído internet es el comercio electrónico, tanto entre empresas y consumidores finales. Dicha tendencia de las nuevas tecnologías, empezó en Estados Unidos, cuando una serie de empresas decidió utilizar internet para desarrollar y expandir sus negocios tradicionales. De esa forma la primera categoría conocida en internet como B2C (Business to Consumer, de negocio a consumidor), es capaz de rebajar costes y reducir el tiempo de suministro. Al cabo de los años aparecieron negocios que su actividad de ventas era exclusivamente por Internet. A partir de aquí, empezaron a salir nuevos modelos de negocio el B2B (Business to Business, de negocio a negocio) y entre otros, mencionados a continuación.

MODELO B2C[6] (Business to Consumer, de negocio a consumidor)

Se define como el contrato comercial realizado a través de internet que se materializa cuando un consumidor o particular visita la dirección web de una empresa y se realiza una venta. Hace referencia a las ventas que se establecen entre una empresa y un usuario final o consumidor con el fin de adquirir un producto o servicio. Los sectores son muy diversos entre ellos (libros, juguetes, viajes, música, ropa).
Las claves de funcionamiento de dicho sector es la efectiva reducción de precios, por no abrir delegaciones, con una dirección accedes a nivel mundial y reducción de costos a nivel de infraestructura. La compañía por referencia del modelo B2C es Amazon, por ser una de las más importantes a nivel mundial en ventas de libros y discos a través de su portal de internet.

MODELO B2B[7] (Business to Business, negocio a negocio)

Es dar servicio de empresas a empresas, generalmente es de mayorista a minorista o autónomos. Dicho modelo B2B son direcciones web destinadas al intercambio de productos y servicios entre empresas que pretenden reducir costos entre ellos. Dichas direcciones generalmente son sitios de acceso restringido y sólo pueden entrar las empresas que tiene acceso con un login y password para poder realizar sus transacciones comerciales. Es un medio para abaratar costes en los procesos de compra, venta, facturación e intercambio de información. Existe

[6] Seoane Balado Eloy. La nueva era del comercio: comercio electrónico. Pág. 4
[7] Ibídem. Pág. 4

englobado en dicho modelo la “empresa virtual”, donde se activan estándares mediante la contratación a empresas especializadas, un ejemplo de viabilidad de dicho modelo son las compañías de General Motors y Ford.

MODELO C2C[8] (Consumer to Consumer, consumidor a consumidor)

Engloba aquellas transacciones en las que tanto como el vendedor y el comprador, son consumidores finales, generalmente se trata de asociaciones de consumidores con intereses comunes, que apoyándose en las infraestructuras existentes, crean entornos que le permiten intercambiar ideas, conocimientos o productos. Por lo tanto en el comercio electrónico C2C los consumidores actúan tanto como compradores y vendedores a través de una plataforma de intercambio. La comunidad en línea eBay con más de 30 Millones de usuarios es otro ejemplo de un comercio electrónico C2C (De consumidor a consumidor), eBay efectuó transacciones por más de 5,000 millones de dólares en el año 2011, se realizan aproximadamente 2 millones de subastas por mes en más de 1000 distintas categorías de artículos o productos.

MODELO C2B[9] (Consumer to Business, consumidor a negocio)

Se basa en una transacción de negocio originada por el usuario final, siendo éste quien fija las condiciones de venta a las empresas. El modelo es muy interesante, existen páginas que los usuarios ofrecen sus casas como alquiler y las compañías de viajes pugnan por dichas ofertas, aquí podemos ver muchas páginas web que se dedican a dicho negocio como pagar noches de hotel, boletos de avión , una cena romántica en una casa rural. Un ejemplo de C2B es la página web Priceline.com.

MODELO M2B (Mobile to Business, móvil a negocio)

Dicho modelo nace para los entornos de Internet móvil (teléfonos, Ipoh, IPhone, etc.), utiliza el teléfono y otros dispositivos móviles para conectar al usuario con la web, fomentando las ventas de muchos productos, sobre todo tonos, juegos, imágenes, música, videos. Gracias a la proliferación de dichos dispositivos las ventas por M2B será el futuro de muchas empresas a nivel comercial. Las nuevas tecnologías como SMS, WAP, GPRS, UMTS y JAVA, serán las que empujen dicho modelo a niveles importantes de comercio. (Anexo 2. Grafica B E-Commerce móvil. Pág. 127)

[8] Seoane Balada Eloy. La nueva era del comercio: comercio electrónico. Pág. 4

[9] M. Siebel Thomas. Principios del E-Business. Pág. 13

2.3 MODELOS DEL COMERCIO ELECTRÓNICO

Actualmente las empresas están descubriendo usos recreativos para el comercio electrónico de negocio a negocio. Esta situación ha generado muchos modelos comerciales nuevos. **Un modelo de negocios es un plan definido para realizar negocios**[10]. Los mercados del lado de las compras y del lado de las ventas fueron los primeros usos que se le dio al comercio electrónico. Para unir grupos de compradores o vendedores, se han creado otros mercados.

2.3.1 TIENDA ELECTRÓNICA (E-SHOP).

El primer paso en el Comercio Electrónico consiste en trasladar a Internet el negocio que la empresa posee en el mundo real. Para ello, la empresa publicará en la red el catálogo de sus productos o de sus servicios. Generalmente, la empresa venderá sus productos agrupados en diferentes categorías de precios, ya que los consumidores tienden a comprobar la calidad del producto y la capacidad del envío antes de pasar a adquirir otros artículos más caros. Los productos que mejor se adaptan a este modelo son los que prácticamente carecen de intangibilidad, como por ejemplo, boletos de avión, entradas de espectáculos, discos compactos, libros, software, herramientas, coches, etc.

Los consumidores esperan que los precios de los productos en línea sean inferiores que los correspondientes a las compras tradicionales. Como ejemplo, los libros en la red suelen venderse con un descuento, o bien no suelen incluir cargos adicionales por el envío.

[10] Oelkers Boen Dotty. Comercio electrónico.. Series Business. Pág. 32

2.3.2. APROVISIONAMIENTO ELECTRÓNICO (E- PROCUREMENT)

Consiste en el uso de nuevas tecnologías que automatizan y optimizan la función de compras de una empresa. El término hace referencia a un intercambio B2B, es decir una transacción entre dos empresas que permite que el comprador consulte en línea el catálogo de productos de un vendedor y haga un pedido de acuerdo con un flujo de trabajo, de compras bien definido. Gracias al aprovisionamiento electrónico, el proceso de solicitud de presupuestos, de emisión de un pedido de compra y de facturación se gestiona electrónicamente y de manera centralizada en las dos empresas, lo que permite acortar los tiempos de pedido y entrega y simplificar el proceso de compras. Por lo tanto, en general, el aprovisionamiento electrónico permite reducir gastos y mejorar el manejo de las compras.

2.3.3. SUBASTA ELECTRÓNICA (E-AUCTION)

La subasta electrónica[11] es un modelo de gran éxito en Internet. Dentro de las categorías de comercio electrónico, puede utilizarse tanto en B2B como en B2C. Y teniendo en cuenta la atención que este modelo genera, puede también integrarse en tiendas electrónicas convencionales.

Los objetos de subasta van desde productos metálicos hasta agrícolas pasando por productos financieros e incluso obras de arte de gran calidad. Al igual que en un CCE (Centro de Comercio Electrónico), una subasta electrónica suele reunir una gran cantidad de vendedores. El responsable de la subasta (cibermediario) suministra los mecanismos necesarios para la exposición de los objetos y para las ofertas (habitualmente a través del correo electrónico), y podría además proveer de mecanismos de pago y de servicios de envío. El cibermediario normalmente cobra un porcentaje prefijado de la transacción al vendedor.

[11] Oelkers Boen Dotty. Comercio electrónico.. Series Business. Pág. 33

2.3.4 CENTRO COMERCIAL ELECTRONICO (ELECTRONIC MALL)

Un centro comercial electrónico es un conjunto de tiendas de productos electrónicos independientes que comparten un entorno de mercadeo electrónico de dichos servidores o software y sistemas de pago. Sito Web que muestra catálogos electrónicos de varios proveedores y gastos de comisión de los mismos para los ingresos por ventas generados en ese sitio.

Beneficios:

- Web donde se agrupan varias tiendas electrónicas
- Marca reconocida, estrategia de marketing (mercadeo)
- Servicios
  - Marketing personalizado
  - Mantenimiento de la tienda
  - Validación de pedidos
  - Varias posibilidades de pago electrónico
  - Servicio de envío de pedidos
- Coste
  - Cuota fija
  - Porcentaje por transacción
    - Por número de artículos, tipo de publicidad

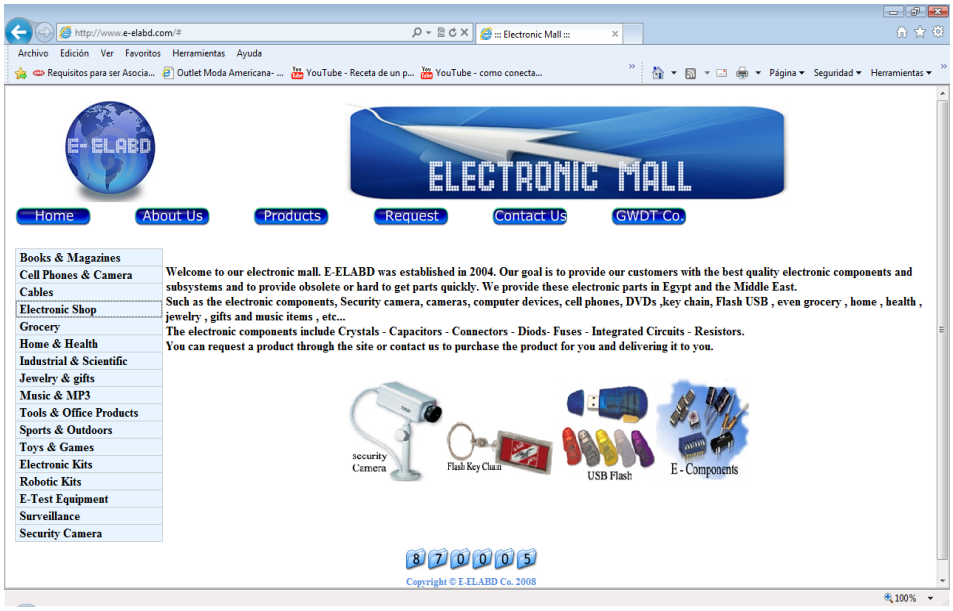


Figura 1.2.- Ejemplo de Electronic mall

2.4 VENTAJAS Y DESVENTAJAS DEL COMERCIO ELECTRÓNICO

La naturaleza global de la tecnología, la oportunidad de llegar a cientos de millones de personas, su carácter interactivo, la variedad de posibilidades para su uso, así como el ingenio y el rápido de crecimiento de sus infraestructuras de apoyo, sobre todo la web.

Ventajas para los usuarios:

- Abarata costos y precios.
- La facilidad de buscar y comprar en el momento.
- Mejores precios al eliminar intermediarios.
- Capacidad de comprar productos y servicios desde un mismo lugar.
- Establecer una relación con el proveedor.
- Bajos costos de transacción.
- Disponibilidad las 24 horas del día, 7 días a la semana, todo el año.
- Un medio que da poder al consumidor de elegir en un mercado global acorde a sus necesidades.
- Reducción de la cadena de distribución, lo que le permite adquirir un producto a un mejor precio.
- Información inmediata sobre cualquier producto, y disponibilidad de acceder a la información en el momento que así lo requiera.
- Permite el acceso a más información.

DESVENTAJAS DEL COMERCIO ELECTRÓNICO

- **Desconocimiento de la empresa.** No conocer la empresa que vende es un riesgo del comercio electrónico, ya que ésta puede estar en otro país o en el mismo, pero en muchos casos las "empresas" o "personas-empresa" que ofrecen sus productos o servicios por Internet ni siquiera están constituidas legalmente en su país y no se trata más que de gente que esta "probando suerte en Internet".

- **Forma de Pago.** Aunque ha avanzado mucho el comercio electrónico, todavía no hay una transmisión de datos segura el 100%. Y esto es un

problema pues nadie quiere dar sus datos de la Tarjeta de Crédito por Internet. De todos modos se ha de decir que ha mejorado mucho.

- **Intangibilidad.** Mirar, tocar, hurgar. Aunque esto no sea sinónimo de compra, siempre ayuda a realizar una compra.

- **El idioma**. A veces las páginas web que visitamos están en otro idioma distinto al nuestro; a veces, los avances tecnológicos permiten traducir una página a nuestra lengua materna. Con lo cual podríamos decir que éste es un factor "casi resuelto".

- **Conocer quién vende**. Ya sea una persona o conocer de que empresa se trata. En definitiva saber quién es, como es, etc. Simplemente es una forma inconsciente de tener más confianza hacia esa empresa o persona y los productos que vende.

- **Privacidad y seguridad.** La mayoría de los usuarios no confía en el Web como canal de pago. En la actualidad, las compras, se realizan utilizando el número de la tarjeta de crédito, pero aún no es seguro introducirlo en Internet sin conocimiento alguno. Cualquiera que transfiera datos de una tarjeta de crédito mediante Internet, no puede estar seguro de la identidad del vendedor. Análogamente, éste no lo está sobre la del comprador. Quien paga no puede asegurarse de que su número de tarjeta de crédito no sea recogido y sea utilizado para algún propósito malicioso; por otra parte, el vendedor no puede asegurar que el dueño de la tarjeta de crédito rechace la adquisición.

2.5 TEORÍAS QUE SUSTENTAN LA INVESTIGACIÓN

2.5.1 OCHO CONSEJOS PARA DETECTAR SITIOS WEB CONFIABLES PARA REALIZAR COMPRAS DE MANERA SEGURA

Los expertos de Seguridad y Privacidad de EDS (Electronic Data Systems**,** es una empresa global de consultoría de tecnologías de la información) recomiendan los siguientes pasos para que los consumidores.

1. Conocer el negocio en el que usted esta comprando.
Si es una compañía que usted no conoce, compruebe que la página Web tenga una dirección física y un número de teléfono. También, verifique que el sitio Web sea miembro de un programa de confianza comercial. Esto certifica que el negocio tiene ciertos estándares comerciales.

2. Asegure que usted esté haciendo compras en un Sitio Web seguro.
Un Sitio Web seguro usa la tecnología de encriptación de códigos de la información que usted envía, por ejemplo el número de la tarjeta de crédito, a fin de impedir que ladrones de identidad tengan acceso. Las direcciones de sitios Web seguras también incluyen https: // a principios de la dirección URL la "**s**" indica que el Sitio Web es seguro. También, busque un candado cerrado en el fondo de su pantalla. Si la cerradura está abierta o no presente, esto puede ser un signo de que el sitio no es seguro. Incluso en un sitio seguro, no envíe ninguna información financiera que no sea necesaria para completar su transacción. Siempre mantenga una copia impresa de su transacción.

3. Verifique los correos electrónicos que aparentemente son confiables.
Los ladrones de identidad se hacen cada vez más sofisticados en sus tentativas de robar la información personal. El Phishing (ladrón de identidad) envía correos electrónicos cada vez más similares a los sitios que ellos tratan de imitar y a menudo se dirigirán a usted por su nombre, haciéndolos más convincentes. Es importante tener cuidado con correos electrónicos que usted reciba de organizaciones que piden información personal (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). Los negocios respetables nunca le pedirán divulgar la información personal, si usted no pidió información antes. Es importante desplegar el sitio Web, en vez de abrir la liga del correo que se recibió. (Anexo 3.Phishing. Pág. 122)

4. Revise pólizas de seguridad y privacidad de las compañías con las que usted hace una transacción.

Todas las compañías respetables publican sus políticas de seguridad y privacidad o una declaración en su sitio Web con el objetivo de conocer cuál es el uso de nuestra información personal y como se usa. Si usted está preocupado por la información compartida con otras compañías, asegúrese de solicitar que su información se mantenga confidencial. Si esta opción no es ofrecida, considere a otra compañía para hacer su compra.

5. Esté consciente que los estándares internacionales de seguridad y privacidad pueden ser diferentes.
Cuando usted hace compras en los Estados Unidos, usted está protegido según leyes del consumidor estatal y federal. Estas leyes pueden no aplicar si usted hace una orden de compra internacional. Si no es una compañía respetable y hay un problema, puede ser difícil que usted lo pueda resolver. Es muy importante conservar una copia impresa y una copia de los términos, condiciones, garantías, descripción del artículo, información de la compañía, la confirmación de los correos electrónicos, y guardarlos con los archivos de su compra.

6. No usar información personal para contraseñas.
Muchos comerciantes en línea ahora requieren que los consumidores registren un nombre de usuario y una contraseña. Esté seguro que sus contraseñas contengan al menos ocho caracteres e incluyen números o símbolos. La utilización de la información como números de cuenta, fechas de nacimiento, nombres, direcciones o números de teléfono hacen que las contraseñas puedan ser un blanco fácil. No anote contraseñas o números personales de identificación para evitar el mal uso.

7. Tener las herramientas de prevención y seguridad actualizadas. Actualice el antivirus y el software de firewall en su equipo de cómputo, y active las aplicaciones de seguridad críticas en su sistema operativo regularmente. Si su software de antivirus no tiene detección de spyware incorporado, compre un explorador de spyware así como un paquete de antivirus. Haga escaneos una vez por semana y elimine cualquier virus no deseado, malware o/y spyware que sea descubierto. Realizar estas actividades con regularidad reducirá dramáticamente los riesgos de algún tipo de ataque.

8. Comprobar su informe de crédito y sus balances de tarjeta de crédito con regularidad. Para asegurar que usted no sea una víctima de robo de identidad, es recomendable verificar sus estados de cuenta regularmente. También debería considerar conseguir acceso electrónico a su tarjeta de crédito y revisar sus cambios periódicamente para asegurar que sus cobros sean correctos y su número de tarjeta no haya sido usado fraudulentamente.

2.5.2 MEDIOS DE PAGOS Y SEGURIDAD A TRAVES DE LA RED

Un **sistema de pago electrónico**[12] realiza la transferencia del dinero entre comprador y vendedor en una compra-venta electrónica. Es, por ello, una pieza fundamental en el proceso de compra-venta dentro del comercio electrónico.

Uno de los problemas más difíciles de resolver es la desconfianza de los consumidores en los medios de pago. Las dificultades en los procesos de reclamos y el reconocimiento de la calidad de las marcas on-line por su corta trayectoria han impuesto un límite en la adopción de los métodos de pago on-line. Uno de los aspectos más llamativos es que los usuarios tienen las mismas resistencias a realizar compras telefónicas, cuando los riesgos son similares. A medida que pasa el tiempo se van creando nuevos mecanismos que facilitaran los procesos de identificación, comprobación, verificación y aprobación. Los medios de pago utilizados en internet (sobre todo en B2C, negocio a consumidor) se pueden dividir en medios de pagos on-line y off-line.

Una **transacción electrónica** [13]no es más que un contrato celebrado mediante medios electrónicos, a través de la red. La mayoría de las transacciones que se hacen por la red, son de compraventa donde el vendedor se obliga a transferir la propiedad de un bien al comprador, y este a pagar un precio.

El **Pago Electrónico**[14] se entiende como cualquier operación de pago realizada con una tarjeta de pista magnética o con un microprocesador incorporado (por ejemplo con una tarjeta de crédito), en un grupo terminal de pago electrónico o terminal de punto de venta.

En Internet los medios tradicionales de pago no son efectivos, pues no es posible asegurar el envío de dinero de manera inmediata y confiable.

Para solucionar ese problema, existen hoy en día los llamados Medios de Pago Electrónico, aceptados en la mayoría, por no decir en la totalidad de tiendas virtuales y páginas de Internet, medios que agilizan las transacciones y procuran brindar la seguridad necesaria para llevar a delante el comercio electrónico.

[12] Cohen Daniel, Asim Enrique. Sistemas de información para los negocios. Pág. 243
[13] Ibídem. . Pág. 245
[14] Ibídem . Pág. 247

2.5.2.1 MEDIOS DE PAGOS ON-LINE

Tarjetas de crédito[15]: El método de pago más utilizado en internet son las tarjetas de crédito, que representan aproximadamente un 60% del mercado de la región. Este método es el más cómodo para los usuarios; sin embargo, la mayoría de los consumidores son desconfiados a entregar sus datos on-line por miedo a fraudes. En la realidad los estándares de seguridad son más elevados a lo que los usuarios piensan. Los sistemas de tarjetas de crédito en Internet funcionarán de forma muy similar a como lo hacen hoy en día. El cliente podrá usar si lo desea su tarjeta de crédito actual para comprar productos en una tienda virtual. La principal novedad consiste en el desarrollo del estándar de cifrado SET (Secure Electronic Transaction) por parte de las más importantes compañías de tarjetas de crédito.

Billeteras virtuales: Las "billeteras virtuales", (conocidas en inglés como online wallets), funcionan de la misma forma que una billetera "real" en su propio bolsillo, con la diferencia de que aquéllas son digitales, es decir, existen sólo en el Internet. En lugar de dirigirse al cajero automático de su banco, retirar el dinero en efectivo y colocarlo en su billetera física real, con una billetera virtual usted abre una cuenta gratis, va a un banco de Internet y transfiere dinero a está para hacer compras por Internet o enviar transferencias virtuales en forma económica e instantánea.

Para usar una billetera virtual tanto usted como el destinatario necesitarán tener previamente algún tipo de cuenta con un banco o una cooperativa de crédito, así como acceso al Internet.

Cómo funciona[16]**:** Usted deposita dinero en la billetera virtual, cargando fondos desde su cuenta de banco. Luego usted emplea estos fondos para pagar al proveedor del servicio un cheque que éste le enviará al destinatario designado por usted. Si su destinatario tiene también una billetera virtual, usted puede enviar dinero directamente a su cuenta y luego su destinatario le solicitará al proveedor de contenidos enviarle un cheque o una transferencia de cable. Normalmente no hay cargos para transferir el dinero y sólo se aplica un cargo nominal (que varía de acuerdo a cada país) para retirar dinero utilizando este método. En la mayoría de las billeteras virtuales usted puede cargar el dinero empleando su tarjeta de crédito VISA o MasterCard, sujeta a los límites de la propia tarjeta y un cargo del 3%.

[15] De Núñez Alberto Fernando, Lugones. Modelos de negocios en internet. Pág. 49
[16] http://www.ahorrando.org/Templates/ah/Content.aspx?id=782

Siempre recuerde ver la tasa de interés que usted pagará en su tarjeta por la transacción.

Un proveedor de “billeteras virtuales” en Internet es PayPal. PayPal es el proveedor más conocido que permite la compra y el pago de productos a través de Internet.

Monederos electrónicos: La **tarjeta monedero**[17] o llamado también monedero electrónico, ha sido el sistema de micro pagos multipropósito más eficiente. Ha servido para aquellas transacciones de bajo monto y alto volumen que requieren gran velocidad y seguridad. El sistema ha permitido a los usuarios pagar más rápido que con efectivo y las transacciones se llevan en menos tiempo. Algunas ventajas:

- Se evita las filas y la congestión en los puntos de pagos.
- Se gana más tiempo.
- Es más fácil, rápido y práctico.
- Da mayor seguridad y control de los pequeños gastos de todos los días.
- Se elimina los problemas del cambio y la falta de monedas.

La tarjeta monedero contiene un chip electrónico que se recarga con dinero y permite pagar productos y servicios deslizando la tarjeta en el lector cuyo importe exacto se descargará o acreditará del chip. Se puede recargar en cualquier establecimiento que tenga una terminal para recibir el pago (tiendas abonando un mínimo establecido). También se puede recargar con tarjeta de débito o crédito.

PayPal: PayPal es una empresa del sector del comercio electrónico, cuyo sistema permite a sus usuarios realizar pagos y transferencias a través de Internet sin compartir la información financiera con el destinatario**,** con el único requerimiento de que estos dispongan de correo electrónico. Es un sistema rápido y seguro para enviar y recibir dinero**.**

Paypal procesa transacciones para particulares, compradores y vendedores online, sitios de subastas y otros usos comerciales. La mayor parte de su clientela proviene del sitio de subastas online eBay, compañía que compró Paypal en Octubre de 2002.

Con PayPal puede:

- Comprar en línea con millones de vendedores.
- Pagar en línea con su saldo de PayPal, cuenta bancaria o tarjeta de crédito.

[17] De Núñez Alberto Fernando, Lugones. Modelos de negocios en internet. Pág. 52

- Realizar el pago rápidamente: no tiene que introducir su información de pago y de envío.
- Recibir pagos por lo que vende en eBay, en su propio sitio web o en avisos clasificados y foros en línea
- Enviar y recibir dinero entre familiares, amigos o particulares.

¿Cuáles son los beneficios de utilizar PayPal?

- **Es rápido**. Los pagos se hacen de manera inmediata, más rápido que mediante el envío de cheques o giros postales.
- **Es privado**. No revela su información financiera a los vendedores.
- **Es global**. PayPal se acepta en todo el mundo y se utiliza para hacer pagos a nivel local e internacional. Acepte numerosas tarjetas de crédito internacionales y locales, tarjetas de débito, transferencias bancarias y pagos de PayPal de compradores de todo el mundo, con más de 150 millones de usuarios en 190 países.
- **Es sencillo**. Envíe dinero a quien quiera con unos pocos clics.
- **Es de confianza**. La prevención del fraude líder en el sector le proporciona seguridad.
- **Es rentable**. Enviar dinero es gratis y PayPal es accesible para todo tipo de empresas.

¿Porqué es PayPal un método seguro para realizar pagos y transferencias de dinero?

Es un método seguro para realizar pagos y transferencias de dinero porque usa tecnología de encriptación SSL de 128 bits para proteger toda la información confidencial y el destinatario nunca recibe datos financieros como el número de tarjeta o cuenta bancaria ni información personal.

Además, ofrece programas de protección, donde el comprador puede pedir la devolución total o parcial de su dinero.

2.5.2.2 MEDIOS DE PAGOS OFF-LINE

La desconfianza de algunos usuarios en las tarjetas de crédito, lo bajos limites de crédito de la población más joven y la baja bancaria en América Latina ha impulsado a los sitios de internet de ofrecer modalidades alternativas de pago.

Efectivo: una forma de muy utilizada es el efectivo contra entrega del producto. La dificultad radica en que exige que haya alguien al momento de la recepción con el dinero para pagar.

Transferencia bancaria: Las transferencias bancarias pueden ser realizadas tanto on-line como off-line dependiendo de la plataforma de pago del sistema e integración con el sistema bancario.

2.5.3 CANDADOS Y CODIFICACIÓN

Los navegadores para internet, como Internet Explorer, colocan un icono en forma de candado en la barra de estado del monitor de tu computadora. Si la página que estás viendo es segura, el candado aparecerá cerrado, si no lo es, el candado aparecerá abierto. Normalmente cuando envías el número de tu tarjeta a un sitio dedicado al C.E, el número de la tarjeta está codificado. Un número codificado es un número cifrado de tal forma que no puede entenderlo nadie que no esté autorizado para utilizarlo. El detallista en realidad no recibe el número de tu tarjeta, sino que se envía a un portal de pago. Ahí el número se decodifica y se transmite a la institución financiera que te ofrece el servicio de tarjeta de crédito para que tu compra sea aprobada.

2.6 MECANISMOS DE SEGURIDAD

Hoy en día Internet juega un papel fundamental en las comunicaciones, en el mundo de los negocios, la información, el entretenimiento, las finanzas, etc. Cada vez más, se desarrollan aplicaciones Web[18], que involucran información de carácter confidencial y que requieren mecanismos de seguridad que garanticen que dicha información no será modificada, sustraída o falsificada por personas ajenas. Esto es, que un sistema Web debe garantizar la autenticidad, integridad y confidencialidad de toda la información involucrada en el sistema.

Una aplicación Web que se diga segura, debe contemplar mecanismos que garanticen que efectivamente ninguna persona ajena al sistema, pueda modificar, obtener o falsificar datos de dicha aplicación Web.

Para lograr las medidas de seguridad necesarias en una aplicación Web, se deben implementar los mecanismos siguientes:

- Seguridad en la transmisión de la información, mediante el uso de protocolos de comunicación seguros y certificados digitales
- Seguridad en los servidores, mediante el uso de firewalls principalmente.
- Seguridad de los datos almacenados en discos, bases de datos o repositorios (información cifrada utilizando criptografía simétrica, sellos de confianza)

Las principales tecnologías referentes a la seguridad de la información son[19]:

- Cortafuegos (Firewall)
- Administración de cuentas de usuarios
- Detección y prevención de intrusos
- Antivirus
- Infraestructura de llave publica
- Capas de Socket Segura (SSL, protocolo de capa de conexión segura)
- Conexión única "Single Sign on- SSO"
- Cifrado
- Cumplimiento de privacidad
- Acceso remoto
- Firma digital

[18]http://www.wikilearning.com/curso_gratis/la_seguridad_en_informatica-comercio_electronico/3625-9

[19] ISACA (2008). *ISACA MANUAL DE PREPARACIÓN AL EXAMEN CISM 2008*. Information Systems Audit and Control Association. Pág-. 17

- Intercambio electrónico de Datos "EDI" y Transferencia Electrónica de Fondos "EFT"
- Redes Virtuales Privadas "VPNs"
- Transferencia Electrónica Segura "SET"
- Informática Forense
- Recuperación de datos
- Tecnologías de monitoreo

Estándares de seguridad de la información

- ISO/IEC 27000-series.- Son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

- ISO/IEC 27001.- Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

- ISO/IEC 17799.- Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como *"la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (acceso a la información)"*.

2.6.1 PROTOCOLOS DE SEGURIDADD

Un **protocolo**[20] es un conjunto de reglas que definen como interactúan las entidades de comunicación, el fin único de todo protocolo es proporcionar un servicio.

Para proporcionar ciertos servicios, algunos protocolos de comunicación necesitan procesar la información que transmiten y reciben. Por ejemplo, los protocolos que proporcionan un servicio de comunicación fiable codifican la información transmitida para poder detectar cuándo han ocurrido errores en la transmisión, de forma que puedan iniciar una acción correctiva. Se desarrollan protocolos que proporcionan servicios de seguridad en redes inseguras. También se introducen protocolos para establecer una asociación de seguridad y para la gestión de claves. Se relacionan estos protocolos de seguridad con los protocolos de seguridad estándares desarrollados para la capa IP- seguridad (IPSec) y para la capa de transporte-capa de sockets segura. SSL (secure Sockets layer) y seguridad de la capa de transporte TLS (transporte layer security).

Los protocolos de seguridad utilizados en la actualidad son los siguientes:

- **SSL (Secure Socket Layer.- protocolo de capa de conexión segura)[21]**

Es un protocolo de seguridad que garantiza que la transmisión de datos entre un servidor y un usurario, o viceversa, a través de internet, sean completamente segura. El protocolo se basa en la utilización de un sistema de cifrado que emplea algoritmos matemáticos y un sistema de claves que solamente conocen el usuario y el servidor. Estas claves permiten la encriptación de los datos para que quien no las tenga no pueda leer su contenido. El cifrado es el proceso de transformación de la información que la hace ininteligible excepto para el destinario original. El cifrado constituye la base de integridad de datos y la privacidad imprescindible para el comercio electrónico. Cuando se conecta a un servidor seguro (https://www...), los navegadores avisan de esta circunstancia mediante un candado de color amarillo en la parte inferior o superior y además permiten comprobar la información contenida en el certificado digital que lo habilita como servidor seguro. SSL permite recoger datos tales como información de datos personales, tarjeta de crédito, etc, en un entorno seguro puesto que la información enviada a través de un formulario seguro es transmitida al servidor de forma encriptada.

[20] Alberto León García. Redes de Comunicación. Conceptos Fundamentales y Arquitectura Básicas. pág. 4
[21] The SSL Protocol, V 3.0, http://wp.netscape.com/eng/ssl3/draft302.txt

Un certificado SSL es un archivo electrónico que identifica de forma exclusiva a personas y sitos web y que permite realizar comunicaciones cifradas. Los certificados SSL funcionan como una forma de credencial o de pasaporte digital. Por lo general el “signatario” de un certificado SSL es una autoridad de certificación (CA), como por ejemplo, la empresa VeriSing, que es uno de los mayores proveedores de confianza de servicios de infraestructura online a nivel mundial. La mayoría de los sistemas operativos, aplicaciones web y hardware de servidores son compatibles con SSL.

Proceso del comercio electrónico

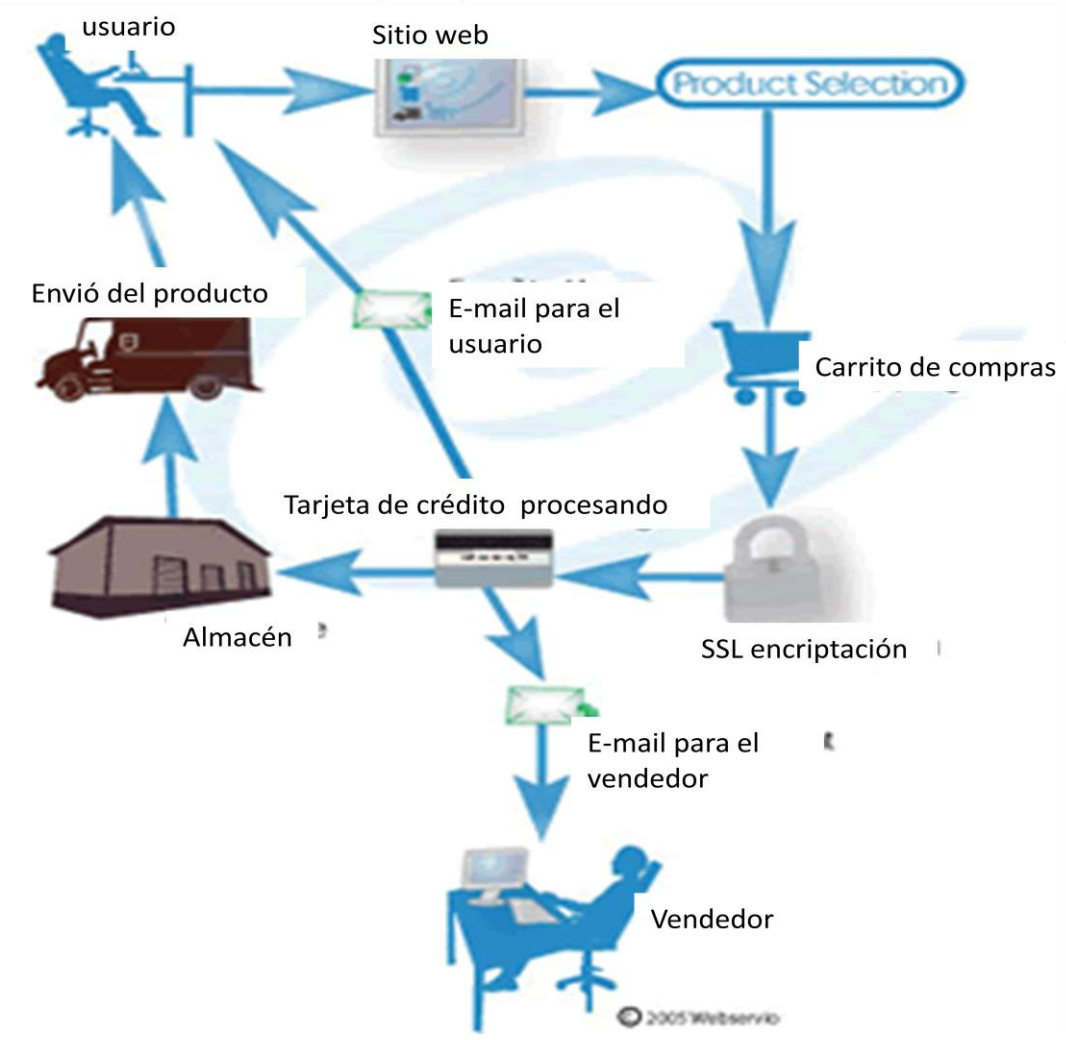


Figura 1.3 Proceso de comercio electrónico

- **TSL (Transport Layer Secure. Seguridad de la capa de transporte)**

Es un protocolo que cifra los mensajes y los entrega de un modo seguro con el fin de prevenir la interceptación y suplantación de identidad entre servidores de correo. Utilizado para establecer seguridad en la capa de transporte del modelo OSI.
TLS utiliza dos mecanismos básicos para garantizar la seguridad del correo electrónico:

1. Cifrado de mensajes: TLS cifra los mensajes entre servidores de correo mediante la infraestructura de clave pública (PKI). De este modo, se dificulta la interceptación y visualización de los mensajes por parte de los hackers.

2. Autenticación de mensajes: la autenticación TLS, que usa certificados digitales, comprueba que los servidores que envían (o reciben) los mensajes son en realidad lo que indica su identificación. De esta forma se ayuda a evitar la suplantación de identidad.

El protocolo TLS[22], es un protocolo para establecer una conexión segura entre un cliente y un servidor, TLS es capaz de autenticar en ambos lados de la comunicación, y crea una conexión cifrada entre las dos.

El protocolo TLS puede ser extendido, esto es que nuevos algoritmos pueden ser utilizados para cualquiera de los propósitos, con la condición de que tanto el cliente como el servidor estén conscientes de los algoritmos. Es utilizado para la encapsulación de varios protocolos de nivel superior, uno de tales protocolos encapsulados, es el TLS Handshake Protocol, el cual es utilizado para autenticar tanto a los clientes como a los servidores, y para negociar un algoritmo de cifrado así como las llaves criptográficas, antes de que el protocolo de la aplicación transmita o reciba el primer byte de datos.

- **Protocolo SET (Secure Electronic Transaction o Transacción Electrónica Segura)**

Este protocolo esta especialmente diseñado para asegurar las transacciones por Internet que se pagan con tarjeta de crédito. Esto es debido a que una gran

[22] Alberto León García, Indira Widjaja. Redes de comunicación. Conceptos fundamentales y arquitectura básicas. 2002. Pág. 4.

cantidad de transacciones de compra por Internet son efectuadas con tarjeta de crédito. El sistema SET fue desarrollado por Visa y MasterCard, con la colaboración de American Express, Microsoft, IBM, Netscape, VeriSign y otras empresas para dotar al comercio electrónico de mayores garantías de seguridad de las que tenía hasta entonces.

Seguridad que proporciona el SET:

- Confidencialidad de los datos de la tarjeta de crédito, ya que al estar el comprador identificado ante la entidad financiera por un certificado digital emitido por ella misma, no es preciso que la información de la tarjeta de crédito viaje, con lo que nunca llega a manos del comerciante ni puede ser interceptada por nadie.
- Integridad de los datos, ya que al viajar encriptados y protegidos por una firma digital no pueden ser alterados en el camino.
- Autenticación del comerciante ante el comprador de que está autorizado para aceptar cobros con tarjetas de crédito.
- Autenticación del cliente ante el comerciante como un legítimo titular de una tarjeta de crédito.

Ahora se muestra un ejemplo del funcionamiento del protocolo SET, con su respectiva descripción. Para darle un mejor entendimiento al tema.

Ejemplo del funcionamiento del Protocolo SET

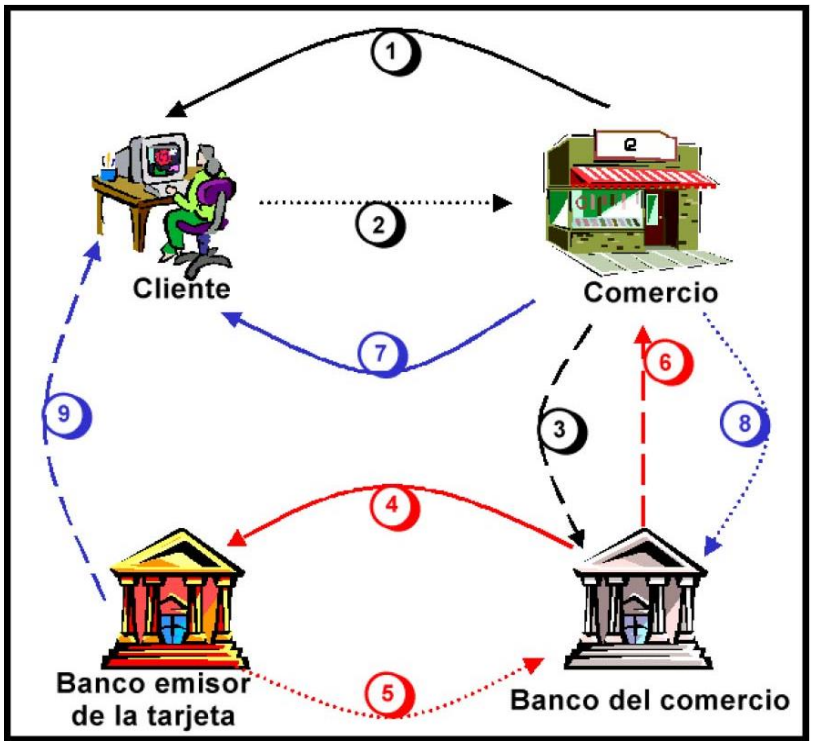


Figura 1.4 – Ejemplo del funcionamiento del Protocolo SET

1) **El cliente inicializa la compra:** consiste en que el cliente usa una página en la red para comprar productos, donde selecciona los productos a comprar y llena la forma de orden correspondiente. **SET** comienza cuando el cliente hace clic en "pagar" y se envía un mensaje de iniciar **SET**.

2) **El cliente usando SET envía la orden y la**

información de pago al comerciante: el software **SET** del cliente crea dos mensajes, uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.

3) **El comerciante pasa la información de pago al banco:** el software **SET** del comerciante genera un requerimiento de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.

4) **El banco verifica la validez del requerimiento**: el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.

5) **El emisor de la tarjeta autoriza la transacción**: el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.

6) **El banco del comerciante autoriza la transacción**: una vez recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.

7) **El servidor del comerciante complementa la transacción**: el servidor del comerciante da a conocer que la transacción que la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.

8) **El comerciante captura la transacción**: en la fase final de SET el comerciante envía un mensaje de “captura” a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.

9) **El generador de la tarjeta envía el aviso de crédito al cliente**: el cargo de SET aparece en estado de cuenta del cliente que se le envía mensualmente.

- **HTTPS (Hypertext Transfer Protocol Secure, Protocolo seguro de transferencia de hipertexto).- utilizado para establecer seguridad en el protocolo HTTP habitual**

El protocolo HTTPS[23] es una versión segura del protocolo http, utiliza un sistema de cifrado basado en la Secure Socket Layers (SSL), para crear un canal seguro cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente, más apropiado para el tráfico de información sensible que el protocolo http, ambos protocolos pueden existir juntos, ya que los navegadores de hoy en día, los soportan.

La idea principal de https es la de crear un canal seguro sobre una red insegura. Esto proporciona una protección razonable contra ataques espionaje e intermediario (*ataque man-in-the-middle* en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado), siempre que se empleen métodos de cifrado adecuados y que el certificado del servidor sea verificado y resulte de confianza. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP (Protocolo seguro de transferencia de hipertexto). Es aquí cuando nuestro navegador nos advertirá sobre la carga de elementos no seguros (HTTP), estando conectados a un entorno seguro (HTTPS).

Los protocolos HTTPS son utilizados por navegadores como: Safari, Internet Explorer, Mozilla Firefox, Opera y Google Chrome, entre otros.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar. El puerto estándar para este protocolo es el 443.

Diferencias con HTTP:

[23] La definición del protocolo HTTP , documento que puede ser localizado en la dirección: http://www.faqs.org/rfcs/rfc2616.html

En el protocolo HTTP las URLs comienzan con "http://" y utilizan por defecto el puerto 80, Las URLs de HTTPS comienzan con "https://" y utilizan el puerto 443 por defecto.

HTTP es inseguro y está sujeto a ataques de espionajes e intermediarios que pueden permitir al atacante obtener acceso a cuentas de un sitio web e información confidencial. HTTPS está diseñado para resistir esos ataques y ser seguro.

- **IPSec (*Internet Protocol security, Protocolo de Seguridad de Internet*)**

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. Mientras que el encriptado puede evitar que un usuario no autorizado pueda leer un mensaje, el autenticado puede evitar los ataques a un sitio originado de sitios externos no deseados o hasta dentro de la propia red del sitio. La seguridad del Protocolo de Internet (IPSec) es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes con el Protocolo de Internet. Los únicos equipos que deben conocer que existe protección con IPSec son el remitente y el receptor de la comunicación. IPSec es autenticación y cifrado a nivel de red, siendo así un estándar abierto para proporcionar comunicación privada y segura. Obligatorio en implementaciones IPv6. IPSec posee dos cabeceras y ofrece una solución flexible y basada en estándares para implementar una política de seguridad en toda una red.

IPsec consta de dos protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 (es la cuarta versión del protocolo Internet Protocol, y la primera en ser implementada a gran escala.) y como para IPv6 (Protocolo Internet Protocol versión 6. Diseñada para reemplazar a IPv4, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet):

- Authentication Header (AH, Autenticación de Cabecera) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.
- Encapsulating Security Payload (ESP, Carga de Seguridad Encapsuladora) proporciona confidencialidad y la opción, altamente recomendable, de autenticación y protección de integridad.

2.6.2 FIREWALLS (CORTA FUEGOS)

El **Firewall**[24] es una herramienta preventiva contra ataques, que realiza una inspección del tráfico entrante y saliente. Esto impide que servicios o dispositivos no autorizados accedan a ciertos recursos y de esta manera protegernos contra ataques de denegación de servicios.

Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

El Firewall puede ser por Software o Hardware o bien combinaciones de estos pero que no serán tratados aquí porque va más allá de esta investigación.

Ventajas de los cortafuegos

- **Establece perímetros confiables.**

- **Protege de intrusiones.-** El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

- **Protección de información privada.-** Permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tenga acceso sólo a los servicios e información que le son estrictamente necesarios.

- **Optimización de acceso.-** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

[24] Turban Efraim. Electronic Commerce 2002. 2002. New Jersey. Pág. 914

2.6.3 QUE ES UN CERTIFICADO DIGITAL

Uno de los problemas al usar servicios online es la falta de seguridad del medio tanto para proteger las transferencias de datos como para asegurar la identidad del usuario. Por estos motivos, se lanzó el concepto de certificado digital**.** Un sistema que permite vincular datos electrónicos con personas físicas a través de una entidad certificadora.

Hoy en día, debido al constante crecimiento de usuarios en Internet y al incremento en las operaciones en línea que se realizan diariamente (comercio electrónico, banca en línea, etc), el tema de seguridad en la red se vuelve cada vez más relevante.

En esta ocasión, explicaremos qué son los certificados digitales, qué contienen y cuáles son sus beneficios.

Un **certificado digital**[25] es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

- La Autoridad Certificadora es una organización confiable que emite o revoca certificados de entidades, mediante la validación y autentificación de dichas solicitudes.
- La llave pública permite cifrar el mensaje enviado (puede ser compartida con cualquier persona), mientras que la llave privada permite descifrarlo (solo tiene acceso el propietario del certificado, misma que puede ser almacenada en una tarjeta inteligente por ejemplo).

Un certificado digital permite identificarse en Internet así como intercambiar información con otras personas o entidades, con la garantía de que sólo quien posee la llave privada puede tener acceso a dicha información. Los certificados digitales son utilizados para aumentar la seguridad de las transacciones en Internet y ayudan a disminuir los fraudes virtuales por suplantaciones de identidad (tanto de personas como de empresas).

Los certificados digitales permiten verificar que la información que se envía es auténtica, es decir que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado (criptograma) no haya sido modificado en su tránsito.

[25] Nash Andrew, Duane William. Joseph Celia, Brink Derek. PIK Infraestructura de claves públicas. La mejor para implementar y administrar la seguridad de su negocio tecnología. Pág. 44

Así pues los certificados digitales, proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, como por ejemplo el envío de correo encriptado, firmas digitales, control de acceso a recursos, la validación oficial de documentos electrónicos, etc.

¿Qué contiene un Certificado Digital?

Existen diversos formatos para certificados digitales, sin embargo los más comunes (utilizados por los navegadores) se rigen por el estándar UIT-T X.509 (*Sector de Normalización de las Telecomunicaciones de la UIT-T* - X.509 es un estándar UIT-T para infraestructuras de claves públicas). Un certificado digital, que vaya de acuerdo al estándar X509v3 (versión 3, Mayo 2008), contiene la siguiente información:

- Identificación del titular del certificado: Nombre, dirección, etc.
- Copia de la llave pública del titular del certificado
- Copia del certificado
- Fecha de validez del certificado (fecha de expiración).
- Número de serie
- Nombre de la Autoridad Certificadora (identificación)
- Firma digital de la Autoridad Certificadora

¿Qué beneficios proporcionan los Certificados Digitales?

El uso de los certificados digitales permite generar la infraestructura necesaria para proporcionar servicio seguros en Internet, y fomentar así el desarrollo del comercio electrónico.

- **Garantizan la integridad de las transacciones y archivos**
- **Garantizan la confidencialidad**
- **Garantizan la autenticidad**
- **Hacen irrefutable una transacción**

Ahora ya lo sabes, con un certificado digital es posible acreditar la existencia de una empresa o persona en la red y asegurar la identidad digital de los sitios web, con el objetivo de realizar envíos de información y transacciones electrónicas seguras y confidenciales.

2.6.3.1 AUTORIDADES DE CERTIFICACION

Una Autoridad Certificadora [26](CA, por sus siglas en inglés) es la encargada de confirmar que el dueño de un certificado es realmente la persona que dice ser. Una Autoridad Certificadora puede definir las políticas especificando cuáles campos del *Nombre Distintivo* son opcionales y cuáles requeridos. También puede especificar requerimientos en el contenido de los campos.

Existen varias Autoridades Certificadoras, puede que una autoridad certificadora certifique o verifique la identidad de otra Autoridad Certificadora y así sucesivamente; pero habrá un punto en que una Autoridad no tendrá quién la certifique, en este caso, el certificado es firmado por uno mismo, por lo tanto, la Autoridad Certificadora es verificada o confiada por ella misma.

Las Autoridades Certificadoras no solamente ofrecen certificados, sino también los manejan; es decir, determinan cuánto tiempo van a ser válidos y mantienen listas de certificados que ya no son válidos (Listas de Revocación de Certificados o CRLS).

Varias compañías se han establecido como Autoridades Certificadoras. Entre las cuales destacan:

- VeriSign, Inc. *[http://www.verisign.com]*
- Thawte Certification. *[http://www.thawte.com]*
- Xcert Sentry CA. *[http://www.xcert.com]*
- Entrust. *[http://www.entrust.net]*
- Cybertrust. *[http://www.baltimore.com]*
- Acepta.com[*http://www.acepta.*com]
- BelSign [http://www.belsign.be]
- Internet Publishing Services *[http://www.ips.es*]

Estas compañías proveen los servicios de:

1. Verificación de solicitud de Certificados.
2. Procesamiento de solicitud de Certificados.
3. Firma, asignación y manejo de Certificados.

[26] Turban Efraim. Electronic Commerce 2002. 2002. New Jersey. Pág. 378

2.6.3.2 CERTIFICADO DIGITAL

Es un recurso electrónico, emitido, respaldado y firmado digitalmente por Symantec. Es una Autoridad de Certificación posicionada como líder mundial en la provisión de productos enfocados a la seguridad en línea. Hace más de un año, Symantec adquirió los Servicios de autenticación e identidad de VeriSign. Se ha invertido en diversas actualizaciones de los certificados SSL y planifica realizar muchas más.

VeriSign es una empresa norteamericana localizada en Dulles, Virginia, que controla 2 de los trece servidores raíz que operan los nombres de dominio primarios punto com y punto net. Es conocida principalmente por emitir certificados de seguridad para su uso en Internet o en aplicaciones informáticas seguras, utilizando protocolos como SSL (Secure Sockets Layer, o Capa de Conexión Segura) y TLS o Seguridad de Capa de Transporte, que codifican la información que se envía a través de redes de todo tipo. Estos protocolos son usados igualmente para acceso seguro a sitios de Internet.

Cómo funciona

Cuando el visitante hace click en el sello instalado en el sitio web, se abrirá una nueva ventana del navegador que mostrará información de su certificado digital incluyendo:

- Su nombre de dominio.
- Estado del Certificado Digital (válido, caducado, revocado) y periodo de validez.
- Información Adicional
- Indicaciones a los usuarios sobre cómo verificar que el sello es autentico..

El sello de seguridad aumenta significativamente el porcentaje de clientes que completan sus compras en el sitio web, al verse respaldados por la seguridad que ofrece VeriSign para realizar transacciones de forma segura

El sello VeriSign Secured Seal, aparece en las paginas web aseguradas por los cetificados SSL de VeriSign. Existen disitintos certificados SSL, con niveles de cifrado y varias opciones de servicos añadidos y garantias.

Figura 1.5 – Ejemplo del Sello VeriSign

Un ejemplo común es cuando realizamos una compra en mercadolibre.com por ejemplo. Me conectaré a http://www.mercadolibre.com/

Estamos en un sitio común, la barra de estado del Internet Explorer nos indica que estamos en un sitio de Internet y la dirección en que estamos ubicados comienza con http://.

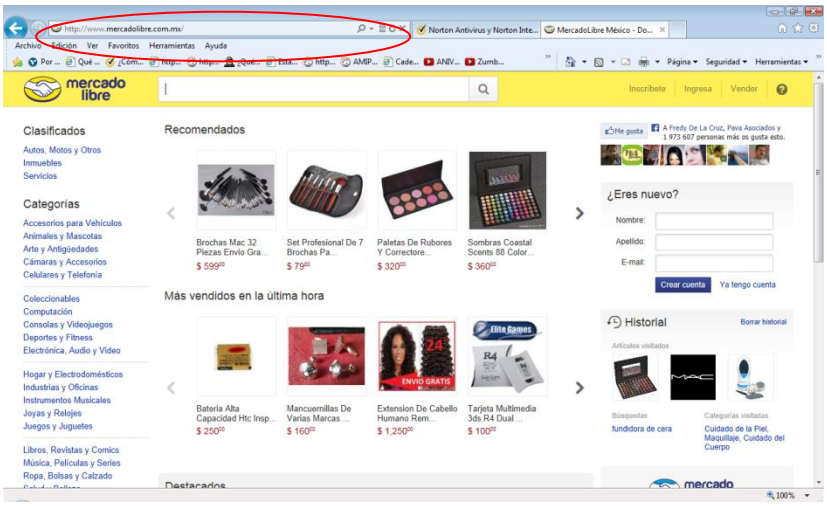


Figura 1.6 – Ejemplo de una página web

Ahora la siguiente pantalla nos mostrará cuando quiero hacer el pago de los del artículo a comprar

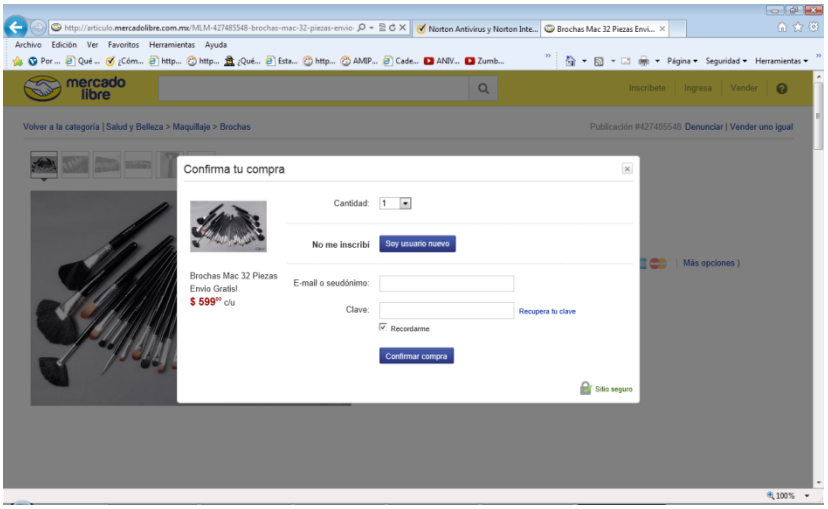


Figura 1.7 – Ventana a la hora de realizar la compra

Ahora un pequeño candado me indica que estoy en un servidor seguro, y que puedo incluir mis datos. Si hacemos click en el candado donde dice Sito Seguro

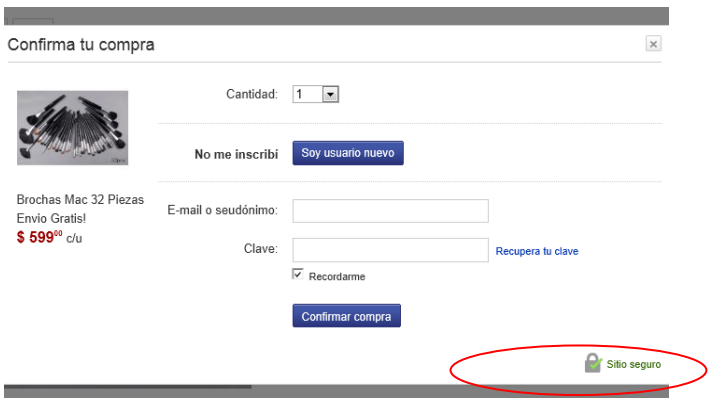


Figura 1.8 – Identificación, Sitio seguro

Nos despliega una nueva ventana donde aparece el sello de seguridad que esta utilizando el servidor de mercadolibre.com.

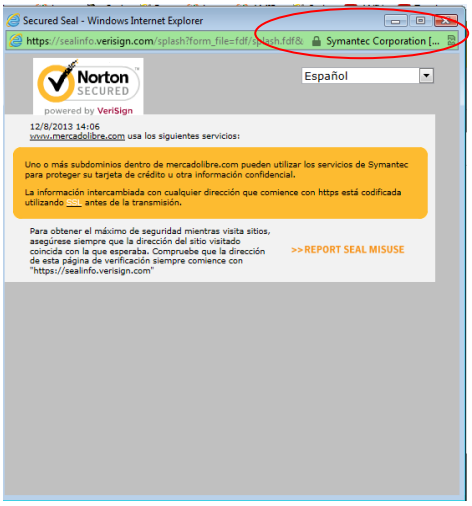


Figura 1.9 – Información del sello de seguridad

Pero si no confiamos, podemos hacer doble clic sobre el candado amarillo y obtendremos información sobre el certificado del servidor de mercadolibre.com.

Esta es la información básica del certificado, que nos confirma que si estamos conectados al sito correcto que es mercadolibre.com y el certificado fue emitido por un CA que es VeriSign o sea una tercera empresa que no tiene que ver nada con la empresa de donde estamos haciendo compras.

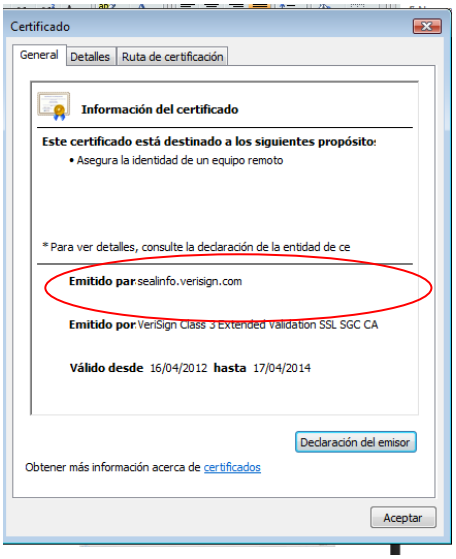


Figura 1.10– Información del sello de seguridad

En esta ventana podemos encontrar información más a detalle sobre el certificado. Como el algoritmo utilizado, la versión de SSL, el algoritmo de identificación, la fecha de valides que posee, entre otros.

La fuerza de cifrado que esta utilizando RSA (2048bits) que es un cifrado muy fuerte.

El 95% de los pagos de Internet se realizan utilizando hoy en día SSL.

SSL no depende de ningún sistema operativo, es independiente, puede ser utilizado sobre cualquier plataforma, independiente.

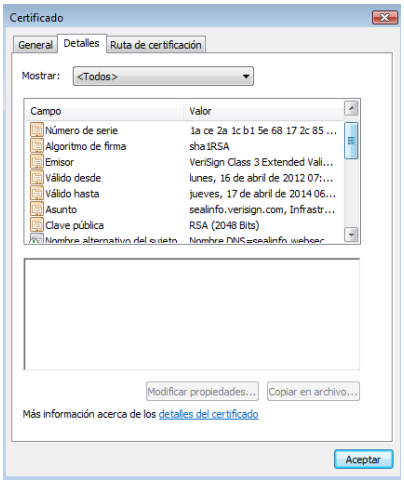


Figura 1.11– Información del sello de seguridad

Los certificados SSL de VeriSign ahora son de Symantec

- **Symantec Secure Site Pro with EV SSL Certificates**

Proteje a sus clientes y haga crecer su empresa con la opción más segura y fiable para la protección de sitios web. Esta solución de seguridad de sitios web incluye Extended Validation (EV), la barra de direcciones verde, y el sello Norton Secured, la marca de confianza más reconocida en Internet. **El cifrado de hasta 256 bits** o de 128 bits, como mínimo.

- **Symantec Secure Site with EV SSL Certificates**

Atrae a más clientes a su sitio web y ofrece la confianza para completar sus transacciones online con Extended Validation (EV), la barra de direcciones verde. Esta solución de seguridad de sitios web también incluye el sello Norton Secured, la marca de confianza en Internet, evaluación de vulnerabilidades y análisis de programas maliciosos en sitios web para ayudarle a tomar medidas contra los puntos débiles importantes de sitios web. **El cifrado de hasta 256 bits** o de 40 bits.

Symantec Secure Site Pro SSL Certificates

Proteja su empresa contra los ataques con el cifrado SSL más fuerte disponible para la mayoría de los visitantes de sitios web. Esta solución de seguridad de sitios web incluye un cifrado de 128 bits verdadero, el sello Norton Secured, evaluación de vulnerabilidades y análisis de programas maliciosos en sitios web para ayudarle a tomar medidas contra los puntos débiles del sitio web.

- **Symantec Secure Site Wildcard SSL Certificates**

Proteja la transferencia de datos confidenciales en múltiples subdominios bajo un solo dominio en su servidor con un único certificado fácil de gestionar. Esta solución de seguridad de sitios web incluye SSL esencial, el sello Norton Secured, la marca de confianza y análisis en busca de programas maliciosos. El **cifrado de hasta 256 bits** protege las transacciones en línea.

- **Symantec Secure Site SSL Certificates**

Proteja la transferencia de datos confidenciales en sitios web, intranets y extranets. Esta solución de seguridad de sitios web incluye SSL esencial, el sello Norton Secured, análisis en busca de programas maliciosos. El cifrado de hasta 256 bits o de 40 bits.

2.6.3.3 TIPOS DE CERTIFICADOS

a) Certificados de autoridades certificadoras[27]

Se utilizan para certificar otro tipo de certificados. Contienen el nombre y la llave pública de la autoridad certificadora, pueden ser auto firmado o firmado por otra organización. Por lo general se incluyen directamente en los navegadores.

b) Certificados de servidores

Contienen la llave pública de un servidor, el nombre de la organización que lo administra, el nombre de anfitrión en Internet y la llave pública del servidor.
Cada servidor que utilice facilidades criptográficas debe tener un certificado de servidor. Cuando el navegador se conecta a un servidor Web mediante el protocolo criptográfico, el servidor le envía su llave pública dentro de un certificado
X.509 v3 el cual autentica la identidad del servidor y distribuye la llave pública que el cliente utilizará para encriptar la información que enviará al servidor.

Un certificado contiene los siguientes campos:

- Longitud de llave de la firma.
- Número de serie del certificado, que es único dentro de cada autoridad certificadora.
- Nombre distintivo.
- Especificación del algoritmo utilizado para la firma.
- Nombre del servidor de dominio.

Los certificados expiran generalmente un año después de su emisión, cuando esto sucede se debe obtener un nuevo certificado. La razón por la que expiran es para disminuir la probabilidad de que la llave privada sea violada y aumentar la confianza en las llaves públicas. Si el navegador se conecta a un servidor Web con facilidades criptográficas y el contenido de un campo del certificado no corresponde con lo esperado, el navegador alerta al usuario o no permite la conexión dependiendo de la configuración de seguridad del mismo.

[27] Nombela José Juan. Seguridad informática. Pág. 232

c) Certificados personales

Contienen el nombre y la llave pública de un individuo, también pueden tener información como su correo electrónico, dirección postal, o cualquier otro atributo de la persona. Los siguientes son algunos de sus usos:

- Elimina la necesidad de nombre de usuario y clave de acceso.
- Se pueden utilizar para enviar correo encriptado.
- Si el certificado contiene datos sobre la persona puede utilizarse para discriminar la información que recibirá.

d) Certificados de editor de software

Se utilizan para firmar software que va a distribuirse. Mejora la confiabilidad del software distribuido por Internet reduciendo la posibilidad de descargar programas hostiles como virus y caballos de Troya.

2.6.4 Garantías de navegación segura: análisis de los sellos y códigos de confianza en comercio electrónico

2.6.4.1. Sellos de confianza

- **¿Qué son los sellos de confianza y garantía de internet?**

Los sellos de confianza son herramientas a través de las cuales las empresas pueden certificar un compromiso ético y responsable de sus actividades comerciales electrónicas, lo que incrementa la confianza y reduce el riesgo percibido por parte de los usuarios y consumidores.

Los sellos acredita, frente al usuario de sito web, que la entidad o empresa que esta detrás cumple con la normatividad y cumple un código de conducta o código ético que persigue la protección y defensa de los derechos de los consumidores. Las empresas que obtienen un sello de confianza consiguen un conjunto de ventajas competitivas respecto al resto de entidades, ya que el distintivo o sello sirve de guía para que los usuarios puedan discernir a aquellos prestadores de servicios que garantizan un elevado nivel de protección de sus derechos, disminuyendo así su riesgo percibido de compra. Los sellos contribuyen a desarrollar una relación de confianza entre el consumidor y la empresa y mejoran la reputación de ésta en un mercado tan amplio como el del comercio electrónico.

- **¿Qué tipo de sellos existen?**

Los sellos son, generalmente, modos de autorregulación que pueden adoptar diversas formas. Entre los sellos existen algunas diferencias que deben tenerse en cuenta respecto al nivel de compromiso que supone su adhesión para la empresa, no sólo en cuanto a su contenido, sino también en cuanto al procedimiento para su concesión.

Por ejemplo, no ofrece las mismas garantías y, por tanto no tiene el mismo reconocimiento social, un sello concedido tras un riguroso procedimiento de auditoría, dirigido a la comprobación del cumplimiento efectivo, por parte de una entidad o empresa, de un estricto código de conducta, que un sello que se concede por la adhesión a una norma pero que no requiere una supervisión o certificación.

Además de los sellos de confianza, existen otros tipos de sellos que reflejan el compromiso hacia diferentes aspectos de la entidad que los han incorporado en su sitios web, como es el caso de los sellos de adecuación o buscadores, sellos de seguridad o sellos de compromiso con la LSSI (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico).

Los sellos de confianza son los más habituales, son instrumentos creados básicamente para aumentar la confianza de los usuarios y disminuir el temor existente a realizar transacciones comerciales a través de internet. En general los sellos de confianza suponen un mayor grado de implicación de la empresa, al tener que cumplir más requerimientos para su obtención. Requerimientos y condiciones establecidas previamente en un código de conducta o ético elaborado por la entidad promotora del sello y cuya obtención suele ser necesario un completo proceso de auditoría.

Otro tipo de sellos, son los que certifican el cumplimiento de una norma. Son comunes los sellos de compromiso LSSI, que garantizan la adecuación del sitio web a lo establecido en la LSSI, la ley 34/2002 de Servicios de la sociedad y la información de comercio electrónico y los sellos LOPD-LSSI que adicionalmente garantizan la adecuación, tanto del portal web como de la empresa titular del domino, a lo establecido en la Ley Organiza de Protección de Datos de Carácter Personal (LOPD).

Existen otros sellos que ofrecen garantías concretas o que sirven para certificar que la web cumple con requisitos técnicos específicos. Es el caso de los sellos de seguridad, que garantizan la protección y seguridad de las transacciones ya que supone que la web ha incorporado soluciones tecnológicas avanzadas que la aseguran.

Por su parte, los sellos de adecuación a buscadores certifican que la página web cumple con determinadas directrices establecidas por los buscadores de internet más habituales, lo que permite que la web tenga más notoriedad y aun mejor posicionamiento en los mismos.

- **¿Que son los códigos de conducta o códigos éticos?**

Los códigos éticos o códigos de conducta o de buenas prácticas comprenden una serie de requerimientos mínimos o reglas que toda empresa que actué en la Red debe cumplir para garantizar la seguridad en las transacciones mercantiles y la protección de los derechos de los usuarios que visitan esos sitios web. Las empresas que quieren obtener un sello de confianza deben adherirse a estos códigos, y se comprometen a cumplirlos voluntariamente. Los códigos ofrecen unas garantías concretas que mejoran o incrementan las reconocidas por el ordenamiento jurídico. También suponen la asunción de unos compromisos específicos, de distinta naturaleza y que dependen de la entidad que los promueve.

Los códigos de conducta incluyen procedimientos independientes para valorar y comprobar que los prestadores de servicios adheridos cumplen las obligaciones

asumidas. Para ello establecen también un régimen sancionador adecuado, eficaz y disuasorio.

La adhesión a un código de conducta, sea cual fuere, ofrece pues derechos y garantías a los consumidores, pero supone que la empresa adquiera una serie de obligaciones.

- **¿Por qué utilizar un sello de confianza en México?**

Porque ya existe en México una ley que regula el tratamiento de datos personales y garantiza la privacidad y el derecho a la autodeterminación informativa de las personas, se trata de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. La cual contempla los Sellos de Confianza como mecanismos de autorregulación en su artículo 44. Asimismo, en el ámbito público, la Ley Federal de Transparencia y Acceso a la Información Pública contempla diversos lineamientos y recomendaciones sobre la protección de datos personales.

- **¿Qué es el Distintivo de confianza en Línea?**

El Distintivo Publico de Confianza en los servicios de sociedad de la información y comercio electrónico, es un sello que se otorga a los prestadores de servicios que se encuentran dentro del marco normativo de la Ley de Servicios de la Sociedad de la Información y estén adheridos a un código de confianza aprobado por el Instituto Nacional de Consumo.

La empresa a la que se le concede, puede incorporar un logotipo o marca tanto gráficamente como por su denominación en todas sus manifestaciones internas y externas, incluida la publicidad. El distintivo pretende servir de guía para que los consumidores y usuarios puedan discernir, dentro del conjunto de sellos y códigos, aquellos que incorporan garantías y un nivel de protección adicional de sus derechos, al estar respaldados por el Instituto Nacional de Consumo.

Para obtenerlo, las empresas deben de adherirse a códigos de conductas cuyos contenidos cumplen una serie de requisitos. Actualmente solo existen tres códigos de conducta aprobados por el INC: El código de Confianza Online y E-Commerce Optima web, promovido por ANETCOM; el código de conducta APTICE de la Asociación para la Promoción de las Tecnologías de la Información y el Comercio Electrónico (APTICE) y el código de conducta de confianza OnLine, promovido por la Asociación para la Autorregulación de la Comunicación Comercial

- **¿Qué beneficios tienen los sellos para el consumidor?**

Los sellos de confianza tienen claras ventajas para los consumidores, entre otras: les da mayores facilidades para seleccionar entre el conjunto de empresas que ofrecen comercio electronico. Incrementa su confianza en la empresa al persibir mayor compromiso con la seguridad y la etica de los negocios.

Les da tranquilidad , al aumentar su confianza en como se van a desarrollar las actividades que va a plantear a traves del portal web. Disminuye el riesgo percibido en un entorno virtual. Obtiene mayor proteccion de sus derechos. Garantiza el cumplimiento de sus expectativas sobre las operaciones realizadas.

- **¿Cuándo visito una pagina web como se que cuenta con un sello?**

Las empresas que cuentan con un sello, pueden incorporar una marca o logotipo de su pagina web que representra el sello graficamente. Algunos incluso se pueden incorporar en todas sus manifestaciones internas y externas de la empres, incluso en la publicidad. En la mayoria de los casos, el consumidor puede obtener informacion sobre el codigo de conducta vinculado al sello de confianza haciendo click en la marca que aparece en la pagina web, incluso, en algunos casos, puede conseguir documentacion especifica sobre el certificado de aprobacion para la actividad empresarial concreta, acceder al sistema de reclamaciones, obtener datos de contacto de la empresa.

Figura 1.12 – Ejemplos de algunos sellos de confianza

2.6.4.2 Sello de Confianza AMIPCI

El Sello de Confianza AMIPCI[28] es un distintivo que se ha otorgado desde el año 2007 por la Asociación Mexicana de Internet (AMIPCI) para sitios de Internet en México, a través de un sello electrónico con un certificado digital adjunto, que reconoce a los negocios o instituciones que promueven el cumplimiento de la normativa de protección de datos personales y privacidad de la información, y están legítimamente establecidos. Desde entonces hemos otorgado más de 600 Sellos de Confianza a diversos sitios de Internet.

La Amipci (Asociación Mexicana de Internet, A.C.) en colaboración directa con la Secretaría de Economía, y en su afán por promover las mejores prácticas en línea en México, crearon y ejecutaron el proyecto de Sellos de Confianza AMIPCI, un mecanismo de autorregulación en materia de privacidad, enfocado principalmente al mercado digital.

Desde entonces, la AMIPCI forma parte de la Asia-Pacific Trustmark Alliance que conjunta a diversos proveedores de Sellos de Confianza a nivel internacional. Asimismo la AMIPCI forma parte del Subgrupo de Privacidad de la Información, perteneciente al Grupo de Manejo de Comercio Electrónico del Foro de Cooperación Económica Asia-Pacífico (APEC).

En México hay 117 empresas que obtuvieron el sello de confianza con AMIPCI.

Figura 1.13 – Empresas que cuentan con sellos de confianza de AMIPCI

[28] https://www.sellosdeconfianza.org.mx/nosotros.aspx

2.7 FUTURO DEL COMERCIO ELECTRONICO

Podemos decir que el futuro del comercio electrónico lo ira determinando el usuario y las empresas, ya que si el usuario realmente se convence de que el internet es el medio ideal para llevar a cabo transacciones electrónicas, las empresas lo único que tendrá que hacer es encontrar la manera de transportar y entregar los valores a través de él, como también los certificados de seguridad que usan. Pero, se está abriendo un nuevo terreno intermedio entre el comercio electrónico y el mundo real, donde los comerciantes podrán sacar provecho del conocimiento sobre sus usuarios, para brindar una mejor experiencia.

Hoy en día, los usuarios resuelven sus inquietudes antes de comprar un producto leyendo blogs con reseñas, usan comparadores de precios para obtener el más bajo, encuentran ofertas en subastas, y finalmente realizan la compra a través de una transacción electrónica con su forma de pago predilecta, cerrando todo el círculo de sus compras de manera virtual. Gracias a la competencia, este proceso y sus herramientas fueron refinándose con los años, hasta lograr una experiencia superior a la que obtendríamos en una tienda real.

Por suerte, la misma tecnología que forzó este cambio de paradigma en el comercio continúa evolucionando, y esta vez podría volver a favorecer a las tiendas comerciales físicas. Para empezar, los dispositivos móviles inteligentes como un iPhone o un teléfono equipado con Android, son capaces de leer los códigos de identificación de los productos y obtener información detallada sobre los mismos, opiniones y comparativas de precios, en cualquier lugar donde estemos. Además, la llegada de computadoras en formatos más ligeros como el iPad, permiten a los comerciantes brindar esta información dentro de sus locales de una forma intuitiva y no invasiva.

En cuestión de tiempo, estos servicios comenzarán a integrarse completamente con nuestros perfiles en línea (Facebook, Twitter, Google, etc) y pondrán a disponibilidad de los comerciantes la información necesaria para ofrecernos los productos que sean más acordes con nosotros. De esta forma, no sólo podrán ser los usuarios quienes activen una capa de realidad aumentada y vean los comercios a su alrededor, sino que los dueños de los mismos podrán visualizar quien es la persona que está entrando a su negocio, y como puede atenderla mejor.

Por último, las transacciones en línea gozan de una altísima credibilidad hoy en día, ya sea a través de nuestra cuenta bancaria o intermediarios como PayPal. Ahora el paradigma es mover todas estas opciones crediticias para reemplazar lo que actualmente llevamos en nuestra billetera: dinero en efectivo y tarjetas de

crédito. Demuestran que esto es viable a corto plazo, y abrirá las puertas a nuevos consumidores y vendedores, para operar de una manera segura y moderna, permitiendo pagar por nuestros productos virtualmente en cualquier lado. Realidad aumentada, perfiles en línea y transacciones móviles, quizás las claves para nivelar la balanza del comercio entre el mundo real y el virtual.

Esto hace pensar que su protagonismo en el futuro será incluso mayor que el que tiene hoy en día. Es igualmente cierto que la evolución futura de este tipo de comercio dependerá de forma directa de la capacidad de garantizar su seguridad mediante certificados, sellos, protocolos y criptografía. El comercio electrónico en México sigue siendo cada vez más relevante y más sostenible, al grado de que cada vez hay más competidores, más usuarios y más alternativas como modelo de negocio, razón que da paso al desarrollo de nuevas estrategias de posicionamiento.

Sin duda el comercio electrónico es algo que poco a poco ha ido ganando terreno y los usuarios ya tienen menos temor de poder hacer compras en línea lo que se ve reflejado en un crecimiento considerable en los ingresos obtenidos. La AMIPCI (Asociación Mexicana de Internet) en conjunto con VISA presentó el estudio AMIPCI de Comercio Electrónico y usuarios 2012 que contempla la dimensión del mercado y los hábitos del comprador en línea. En nuestro país represento en 2012 54,500 millones de pesos; es decir, 4,100 millones de dólares. Se estima que haya un crecimiento del 46% para el cierre del 2013, lo cual representa 79,600 millones de pesos. Algunos de los principales retos dentro del comercio electrónico en México es la falta de información, facilitar los procesos de compras, diversificar los métodos de pagos y generar confianza en el consumidor. El medio de pago mas utilizado por el usuario es la tarjeta de crédito (60%), seguido del depósito en sucursal (31%) y PayPal (28%), mientras que la transferencia electrónica gana terreno (28%), 9% más que en 2011.

El Comercio Electrónico en México aún tiene muchos campos por explotar y, por lo tanto, hará que no sólo sobreviva, sino que alcance un mayor porcentaje de ventas en las empresas mexicanas.

2.8 Marco conceptual

Definición

El marco teórico es la etapa del proceso de investigación en que establecemos y dejamos en claro a la teoría que ordena nuestra investigación, es decir, la teoría que estamos siguiendo como modelo de la realidad que estamos investigando. Recuerde que la teoría no es otra cosa que la realidad descrita con ideas y conceptos verbales (son *constructos* [*construcciones*] de nuestra mente), pero no es la realidad misma.

Ayudará a explicar por qué estamos llevando a cabo un proyecto de una manera determinada. También nos ayuda a comprender y a utilizar las ideas de otras personas que han hecho trabajos similares.

Conceptualización

Variable dependiente:

Analizar y describir, la seguridad.- Explicación detallada y ordenada de como el usuario puede identificar cuando se encuentra dentro de un sitio WEB seguro, en el momento de realizar ciertas consultas a páginas web. Asegurando que la información no esté dañada o alterada por circunstancias o factores externos, haciendo uso de los mecanismos de seguridad.

Variable independiente:

Facilidad e integridad de los usuarios.- Consiste en asegurar que los recursos de información, es la propiedad que busca mantener los datos libres de modificaciones no autorizadas por los usuarios, o circunstancias que permiten conseguir o realizar algo, especialmente el pago de un producto o un servicio, a través del medio de internet, que estos sean realizados y utilizados de manera segura.

OPERACIONALIZACION

Variable independiente	Definición conceptual	Categoría	Indicadores	Items	Escala de Likert
Analizar y describir, la seguridad.	Explicación detallada y ordenada de como el usuario puede identificar cuando se encuentra dentro de un sitio WEB seguro, en el momento de realizar ciertas consultas a páginas web. Asegurando la que información no esté dañada o alterada por circunstancias o factores externos, haciendo uso de los mecanismos de seguridad.	Opinión de usuarios sobre el uso del internet	uso del internet	¿En la actualidad hace usted uso del medio internet? ¿Sabía usted, que por internet existe el medio del comercio electrónico? ¿Considera al Internet como un medio de comercialización, Principalmente Cómo?	5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5)sí, Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5) Una moda 4)Una herramienta de compra-venta 3)Medio de difusión de productos (mercadotecnia) 2)Medio de entretenimiento 1)Otra
		Realizar transacciones por internet	Transacciones por internet	¿Ha realizado consultas a productos y/o servicios que involucren	2)Si 1)No

				transacciones de comercio electrónico (compras, remates, transacciones)? ¿Cuánto? ¿Cuál es su grado de aceptación del comercio electrónico para usted? ¿Ha realizado al menos una vez, alguna transacción por internet (Comprar, vender, pagos de tarjetas, consultas páginas de bancos, transacciones con tarjetas, etc.)? ¿Cada cuanto, realiza transacciones por internet?	5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5)100% 4)75% 3)50% 2)25% 1)0% 5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5)Mucho 4)No mucho

					3) Poco 2)Muy poco 1)Nada
		Calidad del producto comprado por internet	Calidad del producto	¿La calidad del producto y los días de entrega, cumplieron con lo especificado en la página de dicha compra? ¿Considera que los productos que se venden por medio de internet son de buena calidad y de buen costo?	5)Muy alta calidad 4)Alta calidad 3)Neutra calidad 2)Baja calidad 1)Muy Baja calidad 5)Muy alta 4)Alta 3)Neutra 2)Baja 1)Muy Baja
		Las compras son transacciones realizadas en internet	Compras	¿Tuvo algún inconveniente en la página a la hora de realizar la compra? ¿La página que usted consulta para realizar una compra que tanta confianza le brinda?	5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5)Muy alta 4)Alta 3)Neutra 2)Baja

					1)Muy Baja
		Formas de pagos a través de internet	Formas de pago	¿Conoce las formas de pagos que se existen atraves de la red? ¿Cuánto?	2)Si 1)No 5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada

Variable dependiente	**Definición conceptual**	**Dimensión**	**Indicadores**	**Ítems**	**Escala de Likert**
Facilidad e integridad de los usuarios.	Consiste en asegurar que los recursos de información, es la propiedad que busca mantener los datos libres de modificaciones no autorizadas por los usuarios, o circunstancias que permiten conseguir o realizar algo, especialmente el	Seguridad en las transacciones	seguridad	¿Le preocupa la seguridad en las transacciones por internet? ¿Cuándo entra en algún sitio web, le toma importancia a la seguridad de dicho sitio? ¿Conoce los mecanismos de seguridad que se	5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5)Mucho

	pago de un producto o un servicio, a través del medio de internet, que estos sean realizados y utilizados de manera segura			utilizan en el comercio electrónico?	4)No mucho 3) Poco 2)Muy poco 1)Nada
		La inseguridad también se hace presente dentro de este mismo medio.	Inseguridad de los usuarios	¿Le preocupa la inseguridad que existe en el medio de internet?	5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada
		Opiniones sobre experiencias y recomendaciones de los usuarios	Experiencias, Recomendaciones	¿Ha sabido de alguien que tenga una experiencia negativa en la compra o uso de algún servicio de Internet? ¿Recomendaría el uso del comercio electrónico a otra persona?	5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada 5)Mucho 4)No mucho 3) Poco 2)Muy poco 1)Nada

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. ENFOQUE METODOLÓGICO

“La metodología representa la manera de organizar el proceso de la investigación, de controlar los resultados y de presentar posibles soluciones al problema que nos llevará a la toma de decisiones” (Zorrilla y Torres 1992, pág. 65).

En este proyecto la metodología que se usara para el estudio de la investigación, servirá para recopilar la información, analizarla y presentarla. Estos procedimientos servirán para mostrar los resultados del estudio, de una vez que hayan sido recopilados.

3.2 TIPO DE INVESTIGACIÓN

El tipo de investigación que se va realizar para este proyecto de tesis va hacer cualitativa y cuantitativo, porque permitirá examinar los datos de manera numérica, especialmente en el campo de la Estadística.

Es decir de tipo exploratoria (“es el diseño de investigación que tiene como objetivo primario facilitar una mayor penetración y comprensión del problema que enfrenta el investigador (Malhotra, 1997, pág. 87) y explicativa (“Es la explicación que trata de descubrir, establecer y explicar las relaciones causalmente funcionales que existen entre las variables estudiadas, y sirve para explicar cómo, cuándo, dónde y por qué ocurre un fenómeno social” (V. Altamirano, José, 1991, pág. 168).

Es de estudio exploratorio porque, es un tema poco estudiado, el cual es novedoso y desconocido para la ciudadanía. Así también será explicativa, que servirá responder y describir cuales son las causas del problema y soluciones, a implementar**.**

3.3 POBLACIÓN

Población:

Población es la totalidad del fenómeno a estudiar en donde las unidades de población poseen una característica común, la cual se estudia y da origen a los datos de la investigación.

La población a estudiar estará dirigida hacia las personas adultas y jóvenes, que serán objetos de estudio debido a que son quienes manejan más el internet, servirá para conocer cuáles son sus conocimientos hacia el comercio electrónico. El estudio se realizará a los ciudadanos de la Ciudad de Coatzacoalcos y Las Choapas.

3.4. MUESTRA

Muestra:

La muestra es una parte de la población, o sea, un número de individuos u objetos seleccionados científicamente, cada uno de los cuales es un elemento del universo. Se obtiene con la finalidad de investigar, a partir del conocimiento de sus características particulares, las propiedades de la población. La muestra para esté proyecto de tesis será de tipo no probabilística, ya que el estudio se realizara en: ciber's cafés, en algunas empresas y escuelas. Se desarrollará en estos lugares debido a que los jóvenes y las personas adultas es a donde asisten para realizar ciertas tareas. Los resultados obtenidos serán generalizables, pero solo a una parte de la población.

3.5 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

El tipo de técnica que se utilizará para la realización de la investigación será por medio de encuestas, ya que estas cuentan con preguntas normalizadas dirigidas a una muestra representativa de la población, esta nos permitirá conocer estados de opinión o hechos específicos. El tipo de encuesta es por muestreo, porque solo se elegirá una parte de la población, que se estima representativa de la población total, el cual se realizará bajo el diseño de un instrumento para elaborar un cuestionario.

"El cuestionario es una técnica para recopilar datos, que consiste en una serie de preguntas, escritas u orales, que debe responder el entrevistado." (Malhotra, 1997, pág. 317.)

En la investigación del comportamiento disponemos de diversos tipos de instrumentos para medir variables de interés y en algunos casos se pueden combinar dos o más métodos de recolección de los datos. El más común es el escalamiento tipo Likert[29]. Este método fue desarrollado por Rensis Likert a principios de los treinta; sin embargo, se trata de un enfoque vigente y bastante popularizado. "Consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios ante los cuales se pide la reacción de los sujetos a los que se les administra".

Como ya se menciono anteriormente, como instrumento de recolección de datos se utilizara el cuestionario e instrumento de medición el escalamiento de likert, para medir determinadas actitudes que puedan arrojar mayor información con respecto a la investigación realizada.

[29] Sampieri Hernández Roberto. Metodología de la investigación. 2007. Pág. 91.

3.6 APLICACIÓN DE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Hasta ahora, el manejo del comercio electrónico es muy alto su uso. Ya que puede utilizarse en cualquier entorno en el que se intercambien documentos entre empresas: compras o adquisiciones, finanzas, industria, transporte, salud, legislación y recolección de ingresos o impuestos. Pero también es una útil herramienta para hacer negocios, pero los fraudes han puesto en duda su desarrollo.

La aplicación del instrumento que se utilizara será aplicada en la Ciudad de Coatzacoalcos y Las Choapas, en diferentes lugares de estas localidades. El cual se aplicara a personas adultas y jóvenes. Estará dirigido a ellos, porque son el mayor porcentaje de personas que utilizan ahora el comercio electrónico o los que están más activos en los sitios webs.

El cuestionario estará compuesto por preguntas estructuradas. Este tendrá como objetivo, ver cuáles son los problemas, los miedos por los cuales, existe la inseguridad para acceder a entrar al mundo del comercio electrónico.

3.7 ANÁLISIS DE LOS DATOS

El análisis de datos es el precedente para la actividad de interpretación. La interpretación se realiza en términos de los resultados de la investigación. Esta actividad consiste en establecer inferencias sobre las relaciones entre las variables estudiadas para extraer conclusiones y recomendaciones.

También es la actividad de transformar un conjunto de datos con el objetivo de poder verificarlos muy bien dándole al mismo tiempo una razón de ser o un análisis racional, según la cual el análisis del contenido es una técnica de investigación para hacer inferencias reproductibles y válidas de los datos.

De acuerdo con los resultados obtenidos de la encuesta realizada por medio de un cuestionarios, en las ciudades de Coatzacoalcos y Las Choapas, en diferentes lugares. Se analizará la información y se realizará, un estudio estadístico, para poder realizar gráficas, en donde se representaran los resultados que se obtuvieron del estudio. Este se realizará bajo el instrumento de medición que es el escalamiento tipo Likert. Cada elemento será separado para poderlo estudiar individualmente. La finalidad de la recolección de datos, es aportar información verídica, oportuna y de relevancia, para la elaboración de propuestas o sugerencias de mejora como objetivo de esta investigación.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN

4.1 CUADROS

A continuación se presenta en cuadros, la información que se obtuvo por medio de la encuesta aplicada. Detallándose en cada cuadro su información correspondiente.

1.- ¿En la actualidad hace usted uso del medio internet?

Se puede observar, que en la actualidad los la mayoría de los usuarios, hacen del uso del medio de internet.

RESPUESTA	No. PERSONAS
5) Mucho	18
4) No mucho	2
3) Poco	3
2) Muy poco	0
1)Nada	0

2.- ¿Sabía usted, que por medio de internet existe el medio del comercio electrónico?

Se observa, dentro de la información recabada que la mayor parte de los usuarios, tienen conocimiento sobre el medio del comercio electrónico, son muy poco los usuarios los que no conocimiento sobre este medio.

RESPUESTA	No. PERSONAS
5) Mucho	17
4) No mucho	4
3) Poco	2
2) Muy poco	0
1)Nada	0

3.- ¿Considera al Internet como un medio de comercialización, Principalmente Cómo?

Dentro de esta pregunta, se obtuvieron diferentes respuestas, dentro de las cuales los usuarios, para la mayoría es una herramienta de compra-venta, para otros un medio de difusión de productos. Otros usuarios lo definieron como, un medio completo de comercio electrofónico, medio de información, un recurso de para comprar libros y como un medio de comunicación.

RESPUESTA	No. PERSONAS
5)Una moda	0
4)Una herramienta de compra-venta	9
3)Medio de difusión de productos (Mercadotecnia)	5
2)Medio de entretenimiento	2
1) otra	7

4.- ¿Ha realizado consultas a productos y/o servicios que involucren transacciones de comercio electrónico (compras, remates, transacciones)?

Se observa, que la mayoría de los usuarios si han realizado consultas que involucran transacciones dentro del comercio electrónico.

RESPUESTA	No. PERSONAS
2)Si	20
1)No	3

5.- ¿Cuánto?

Relacionada con la pregunta anterior, se obtuvo, que la mayoría de los usuarios, son pocas las consultas que realizan y pocos usuarios los que realizan muchas consultas o transacciones.

RESPUESTA	No. PERSONAS
5) Mucho	6
4) No mucho	4
3) Poco	7
2) Muy poco	3
1)Nada	3

6.- ¿Cuál es su grado de aceptación del comercio electrónico para usted?

Se obtuvo, que el grado de aceptación del comercio electrónico para los usuarios es de un 75%, son para pocos el 100% de aceptación. Para el 50% y 25%, fue pareja la aceptación.

RESPUESTA	No. PERSONAS
5)100%	3
4) 75%	14
3) 50%	3
2) 25%	3
1)0%	0

7- ¿Ha realizado al menos una vez, alguna transacción por internet (Comprar, vender, pagos de tarjetas, consultas páginas de bancos, transacciones con tarjetas, etc.)?

De acuerdo a los resultados de esta pregunta, se obtuvo, que la mayoría de los usuarios han realizado varias transacciones como pudo ser, comprar, vender, realizar pagos por con tarjetas de créditos, entro otra. Para otros han realizados pocas y muy pocas transacciones.

RESPUESTA	No. PERSONAS
5) Mucho	6
4) No mucho	6
3) Poco	4
2) Muy poco	3
1)Nada	4

8.- ¿Cada cuanto, realiza transacciones por internet?

Se puede notar, en los resultados obtenidos, que, pocos usuarios son los que realizan siempre transacciones, y la mayoría cae dentro de un periodo 3 semanas hasta 6 meses en realizar al menos una transacción.

RESPUESTA	No. PERSONAS
5) Mucho	2
4) No mucho	7
3) Poco	6
2) Muy poco	3
1)Nada	4

9.- ¿La calidad del producto y los días de entrega, cumplieron con lo especificado en la página de dicha compra?

Para los usuarios que han realizado una transacción dentro de una página web, para la algunos de los usuarios que realizaron dicha transacción, la página cumplió con lo especificado en la compra, para la mayoría fue neutra su satisfacción dentro de la calidad y los días de entrega del producto.

RESPUESTA	No. PERSONAS
5)Muy alta	5
4)Alta	7
3)Neutra	9
2) Baja	0
1)Muy Baja	2

10.- ¿Considera que los productos que se venden por medio de internet son de buena calidad y de buen costo?

Con los resultados obtenidos, se puede observar que la mayoría de los usuarios califico como de neutra calidad y alta calidad, a los productos que venden por medio de internet, pocos son los usuarios que califican los productos como de muy alta calidad.

RESPUESTA	No. PERSONAS
5)Muy alta calidad	3
4)Alta calidad	9
3)Neutra calidad	11
2) Baja calidad	0
1)Muy Baja calidad	0

11.- ¿Tuvo algún inconveniente en la página a la hora de realizar la compra?

En la aplicación de la encuesta, los usuarios dieron sus opiniones, sobre las páginas que han comprado, como mercado libre, de remate, PC en línea, entre otras. Opinaron que son pocas las inconvenientes que tuvieron, pero fueron más por cuestiones del vendedor, que por conflictos de la página.

RESPUESTA	No. PERSONAS
5) Mucho	0
4) No mucho	4
3) Poco	2
2) Muy poco	2
1)Nada	15

12.- ¿La página que usted consulta para realizar una compra que tanta confianza le brinda?

La mayoría de los usuarios opinaron que es neutra la confianza que le brindan a la página en la que realizan sus compras, pocos usuarios es muy alta la confianza.

RESPUESTA	No. PERSONAS
5)Muy alta	5
4)Alta	4
3)Neutra	12
2) Baja	2
1)Muy Baja	0

13.- ¿Conoce las formas de pagos que se existen atreves de la red?

Se puede observar, dentro de los resultados obtenidos, que la mayoría de los usuarios si conocen las formas de pago que existen a través de la red

RESPUESTA	No. PERSONAS
2)Si	22
1)No	1

14.- ¿Cuánto?

Relacionada con la pregunta anterior, se obtuvo, que la mayoría de los usuarios es muy alta y alta el grado de conocimiento de las formas de pagos que existen a través de la red, y para otros

RESPUESTA	No. PERSONAS
5)Muy alta	8
4)Alta	9
3)Neutra	3
2) Baja	2
1)Muy Baja	1

15.- ¿Le preocupa la seguridad en las transacciones por internet?

Para la mayoría de los usuarios si les preocupa mucho la seguridad en las transacciones, opinaron que no conocen mucho sobre los mecanismos de dicha seguridad. Para poco no es mucha su importancia.

RESPUESTA	No. PERSONAS
5) Mucho	16
4) No mucho	2
3) Poco	5
2) Muy poco	0
1)Nada	0

16.- ¿Cuándo entra en algún sitio web, le toma importancia a la seguridad de dicho sitio?

RESPUESTA	No. PERSONAS
5) Mucho	13
4) No mucho	7
3) Poco	2
2) Muy poco	1
1)Nada	0

Se observa dentro de los resultados que la mayoría de las personas encuestadas es muy alta la importancia, de la seguridad que toman encuentra a la hora de entrar a dichos sitios. Para otros sus repuestas fueron variadas donde no es mucha si importancia sobre la seguridad.

17.- ¿Le preocupa la inseguridad que existe en el medio de internet?

La mayoría de personas encuestadas opinaron que es muy grande su preocupación de la inseguridad que existe dentro del internet. Y que les gustaría saber, como identificar estos problemas. Fueron pocas las personas a las que no les preocupa la inseguridad.

RESPUESTA	No. PERSONAS
5) Mucho	16
4) No mucho	6
3) Poco	1
2) Muy poco	0
1)Nada	0

18.- ¿Conoce los mecanismos de seguridad que se utilizan en el comercio electrónico?

Dentro de los usuarios encuestados, se obtuvo que la mayoría de ellos si conocen los mecanismos de seguridad que se utilizan en el comercio electrónico. Menos de la mitad de los usuarios no tienen conocimientos sobre dichos mecanismos.

RESPUESTA	No. PERSONAS
2)si	15
1)No	8

19.- ¿Cuánto?

Relacionada con pregunta anterior, se puede observar que sus conocimientos sobre los mecanismos de seguridad, son muy bajos. Pocos usuarios son los que si tienen un alto conocimiento.

RESPUESTA	No. PERSONAS
5) Mucho	4
4) No mucho	5
3) Poco	4
2) Muy poco	2
1)Nada	8

20.- ¿Ha sabido de alguien que tenga una experiencia negativa en la compra o uso de algún servicio de Internet?

Se puede observar que la mayoría de los usuarios, no conocen sobre experiencias negativas en compras o el uso de algún servicio de internet, son pocos los que si conocen sobre experiencias negativas, sin saber cuáles fueron las causas de estas.

RESPUESTA	No. PERSONAS
5) Mucho	3
4) No mucho	2
3) Poco	6
2) Muy poco	4
1)Nada	8

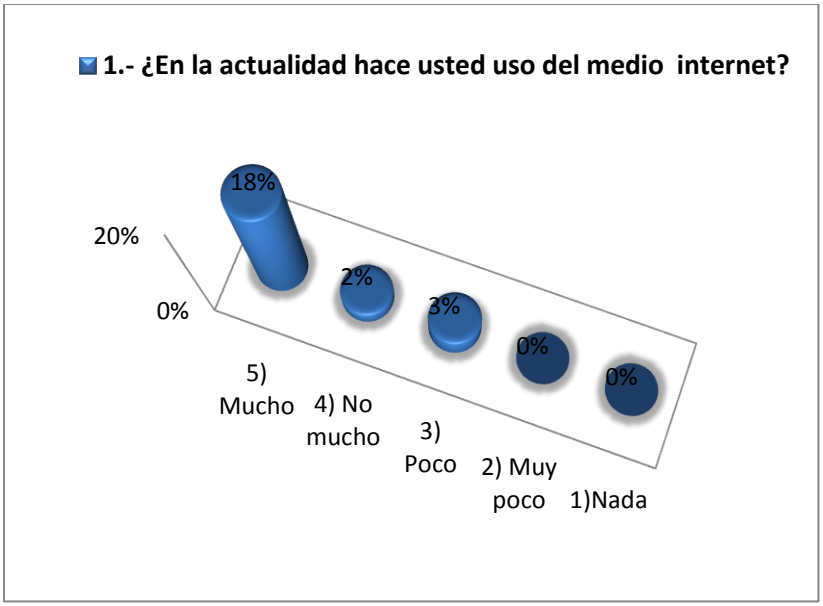
21.- ¿Recomendaría el uso del comercio electrónico a otra persona?

La mayoría de las personas encuestadas, si recomendarían mucho el uso del comercio electrónico, y para otras seria no sería mucha su recomendación.

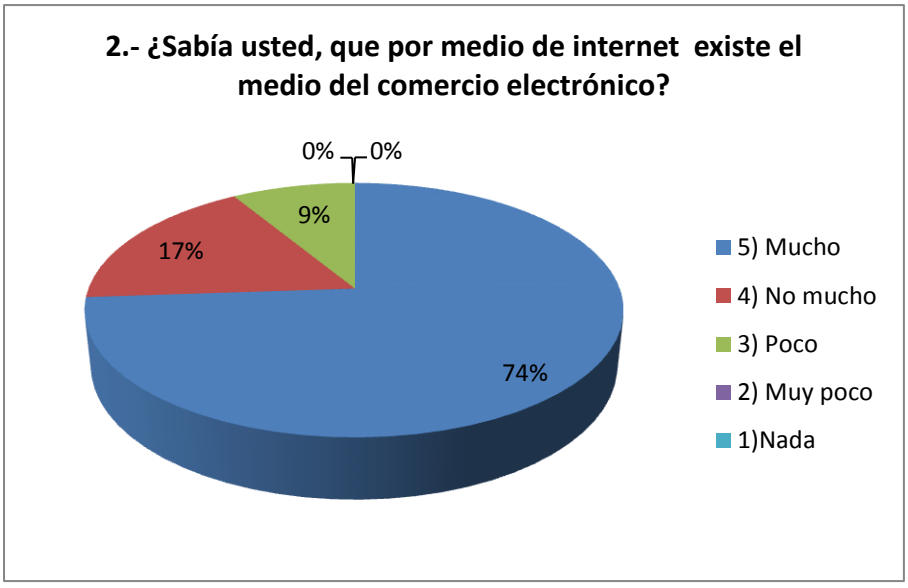
RESPUESTA	No. PERSONAS
5) Mucho	10
4) No mucho	7
3) Poco	3
2) Muy poco	3
1)Nada	0

4.2 GRÁFICOS

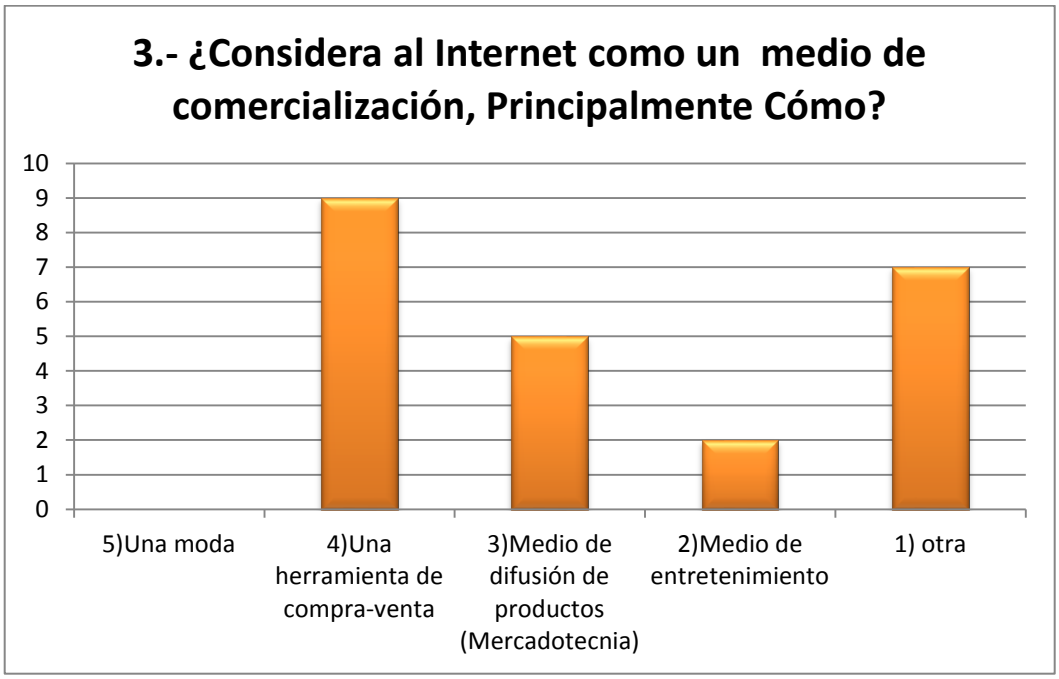
A continuación se presentan los resultados, graficados de acuerdo a la información recopilada por medio de encuestas. Tomando en cuenta cada una de las opiniones de los usuarios encuestados.



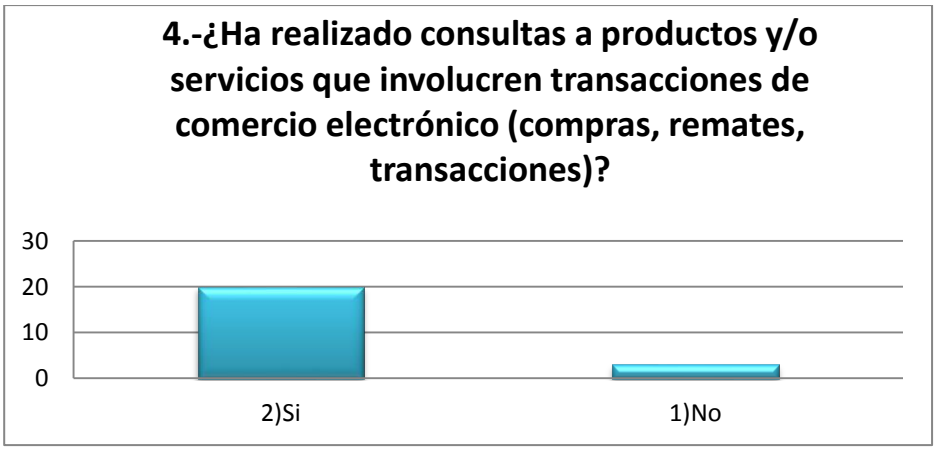
En la gráfica se puede observar, que el 78% corresponde a que la mayoría de los usuarios hacen un mayor uso del medio de internet.



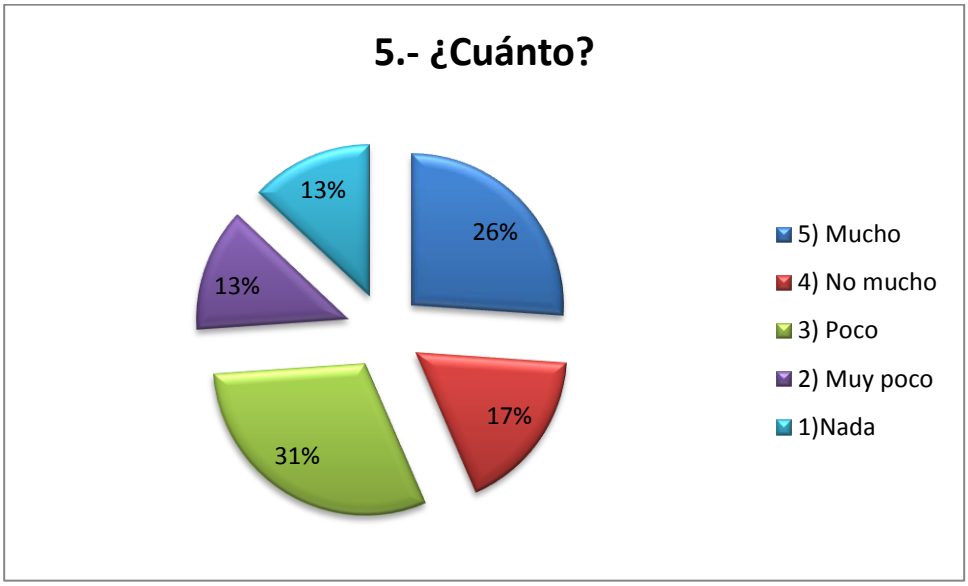
Se observa, dentro de la gráfica, que un porcentaje mayor de 74% de usuarios encuestados conocen, sobre la existencia del comercio electrónico, el 17 % no es mucho, y un 9% poco.



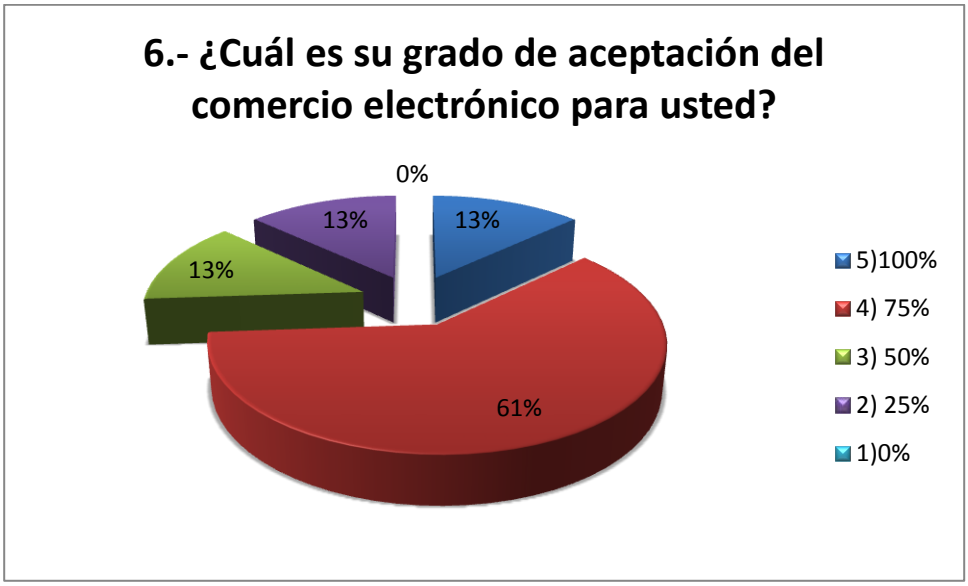
Dentro de la gráfica, se puede observar que de los 23 usuarios encuestados, la mayoría de los usuarios consideran al internet, como una herramienta de compre-venta, 5 usuarios opinaron que es un medio de difusión de mercadotecnia, 2 usuarios como un medio de entretenimiento y 7 usuarios como otra, como medio de información, de comunicación, entre otros.



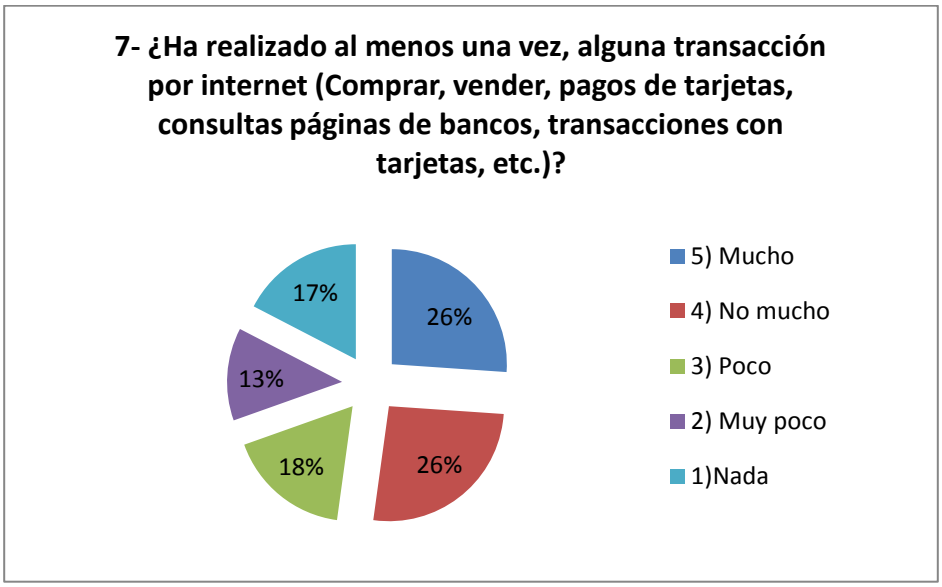
Dentro de la gráfica, se puede observar, que de las 23 personas encuestadas 20, contestaron que Sí, han realizado al menos una consulta de algún producto o servicio, el cual esta involucrado dentro del medio de comercio electrónico.



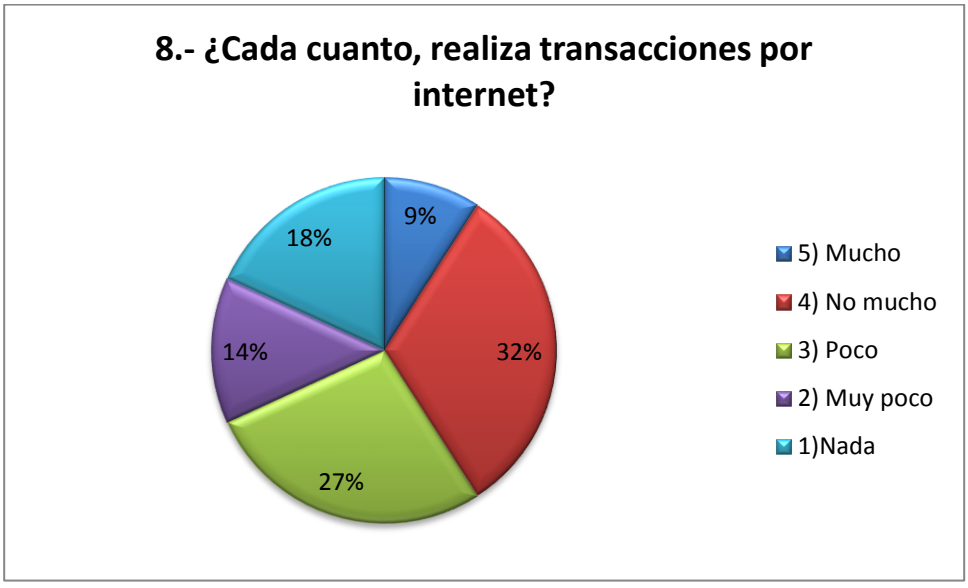
De acuerdo con la pregunta anterior, se puede observar que gráficamente el 31% de los usuarios, son pocas las consultas que han realizado consultas dentro del comercio electrónico, y el 26% son los que han realizados mas consultas dentro de este mismo medio.



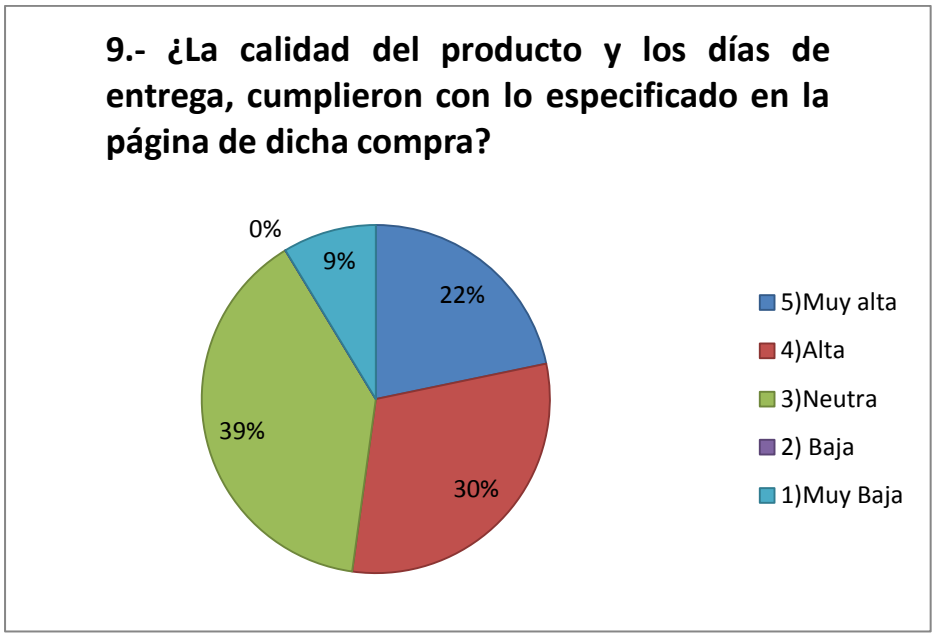
Se observa que gráficamente el 61% de los usuarios su grado de aceptación es del 75% y que solo el 13% de estos es del 100% el grado de aceptación, y el 13% son para el 50% ye 25% de aceptación.



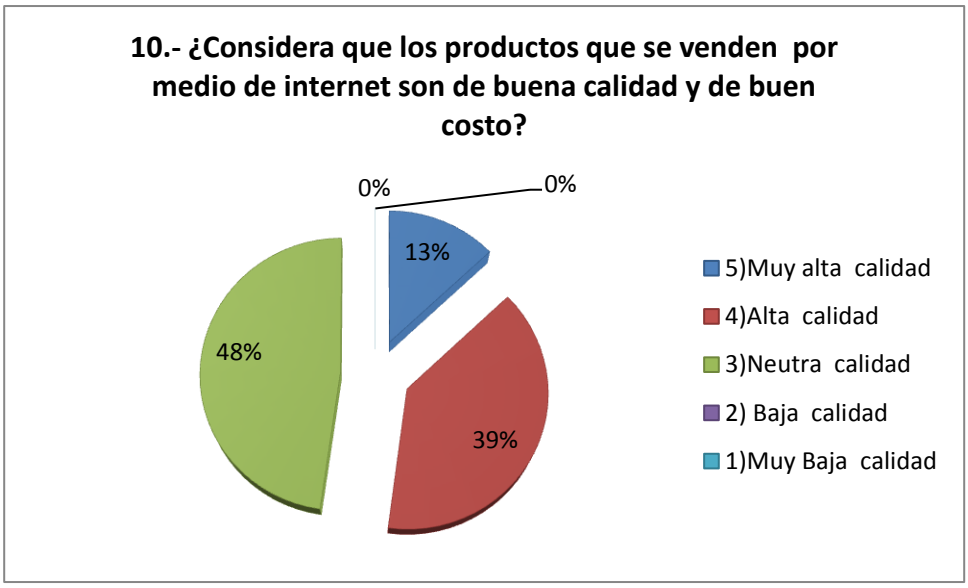
El 26% de los encuestados han realizado muchas transacciones como comprar, vender, pagos con tarjetas entre otros, y otro 26% no es mucho sus transacciones. Y un 17% nunca han realizado al menos una transacción.



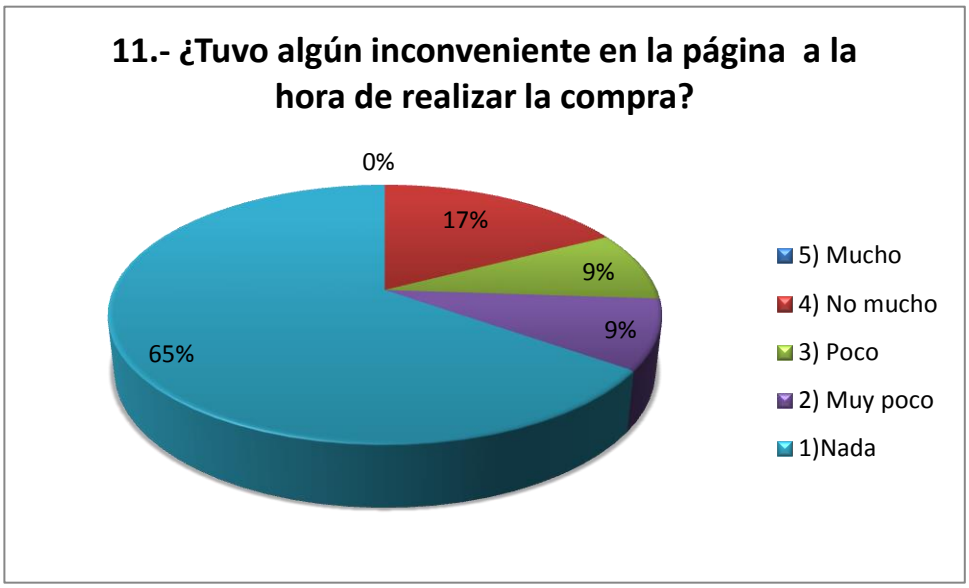
El 32% de los usuarios, realizan mucha transacciones por internet, el 27 % es poca la realización de transacciones, y solo el 14% no realizan nunca transacciones.



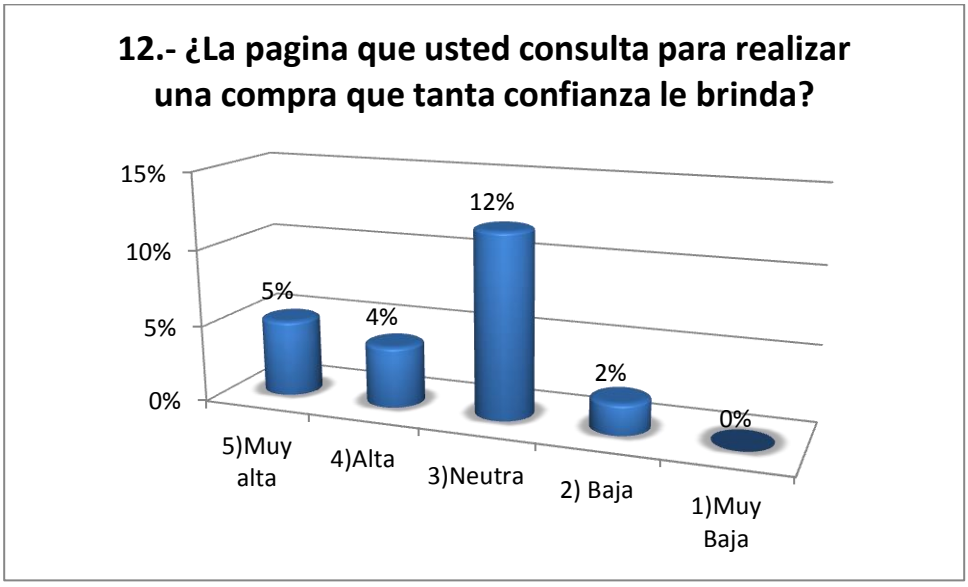
El 39% de los usuarios calificaron como neutra la calidad del producto y los días de entrega, que hicieron con dichas compras, y un 30% como alta la calidad.



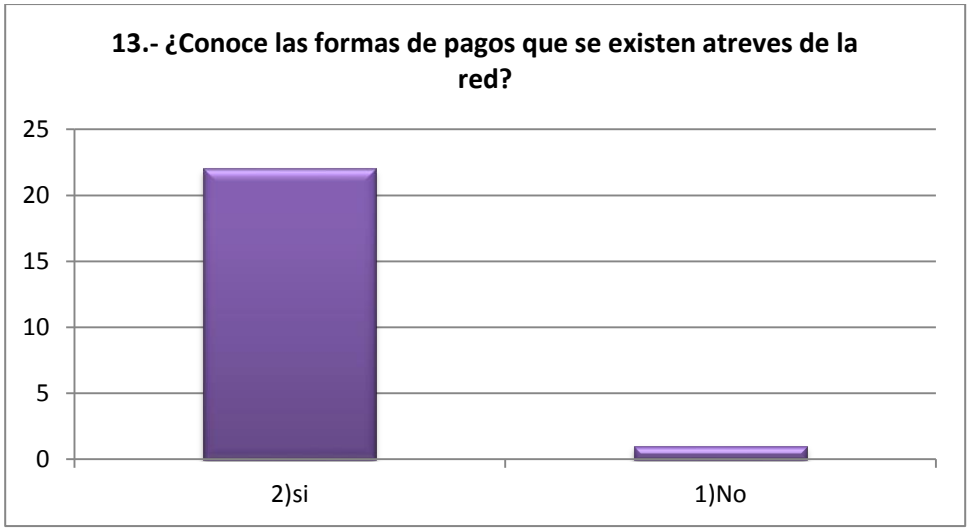
Se puede observar gráficamente que el 48% de los usuarios encuestado, considera de neutra calidad y de buen costo los productos que venden por medio de internet, un 39% los considera de alta calidad y solo un 13% de muy alta calidad y buen costo.



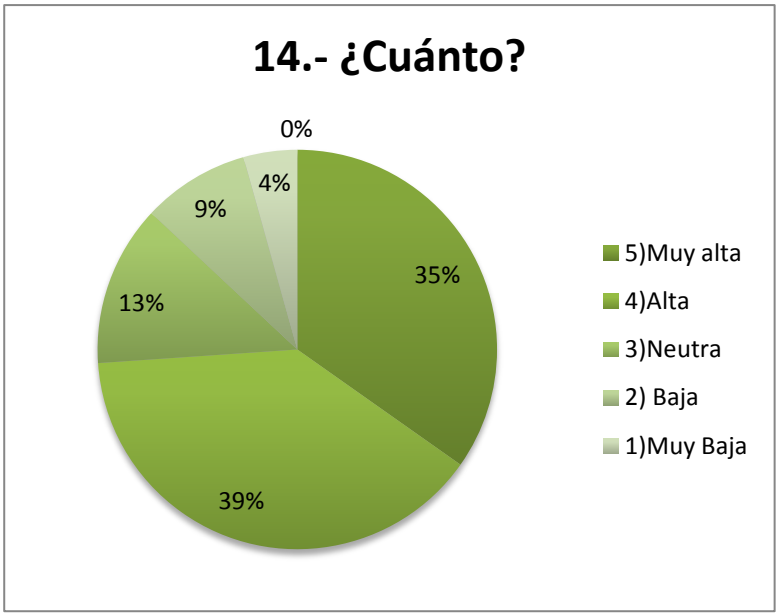
Gráficamente se puede observar que un 65% de los usuarios encuestados opinaron que no tuvieron ningún inconveniente en la página a la hora de realizar una compra, y un 17% su respuesta fue no mucho, pero tomando en cuenta que los inconvenientes fueron por los vendedores, y no en la página.



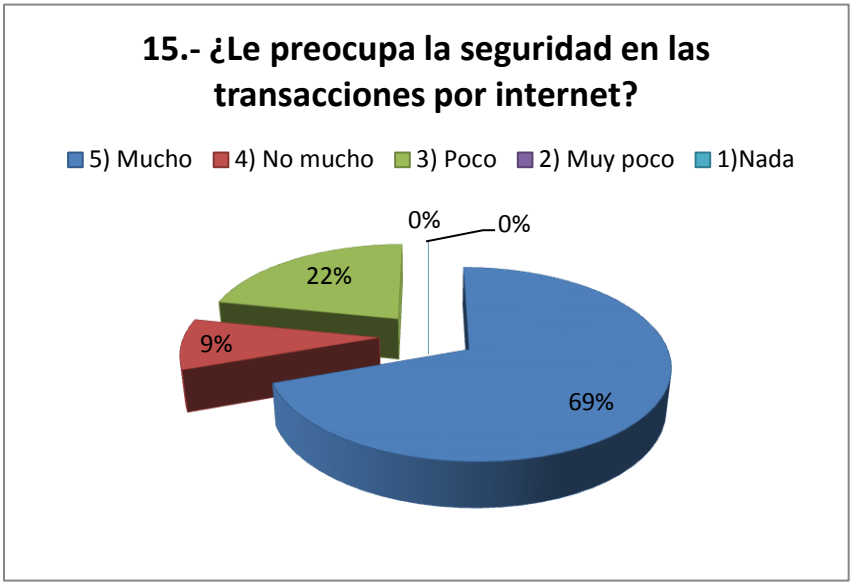
Para los usuarios encuestados el 52% opinaron que es neutra su confianza hacia la página en la que realizan alguna compra por internet, y un 17% es alto la confianza, y para el 22 % es muy alta la confianza que les brinda dicho sito web.



Se puede observar dentro de la gráfica que de las 23 usuarios encuestados, 22 de ellos contestaron que, sí conocen, las formas de pago que existen dentro de la red, solo 1 persona desconoce estas formas de pago. Comentaron que les gustaría conocer más sobre los funcionamientos de dichos pago.

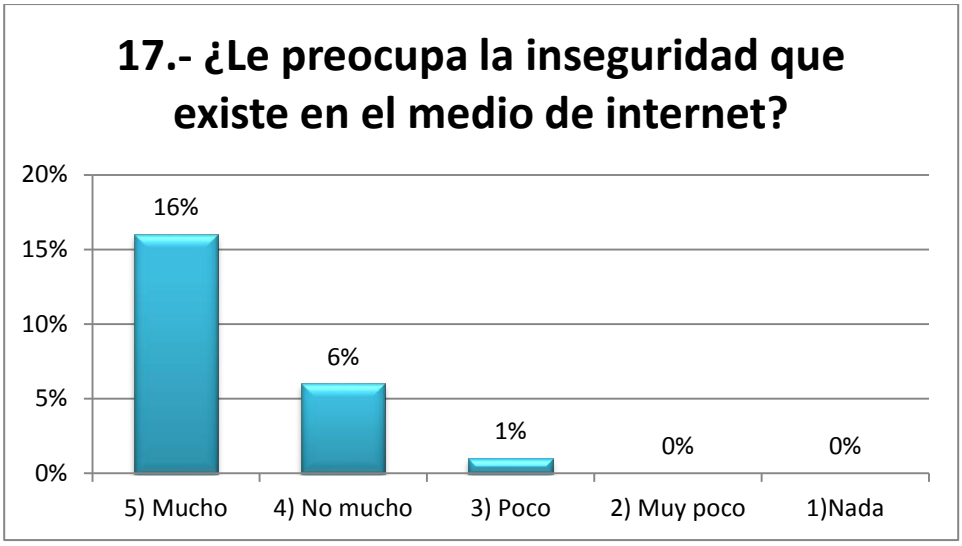


Esta gráfica esta relacionada con la pregunta anterior, de acuerdo con las formas de pago, para el 39% de los usuarios son neutros sus conocimientos, y para el 35% es alta, solo de un 4% a un 9% de ellos, son los que en realidad no conocen mucho sobre las formas de pago atraves de la red.

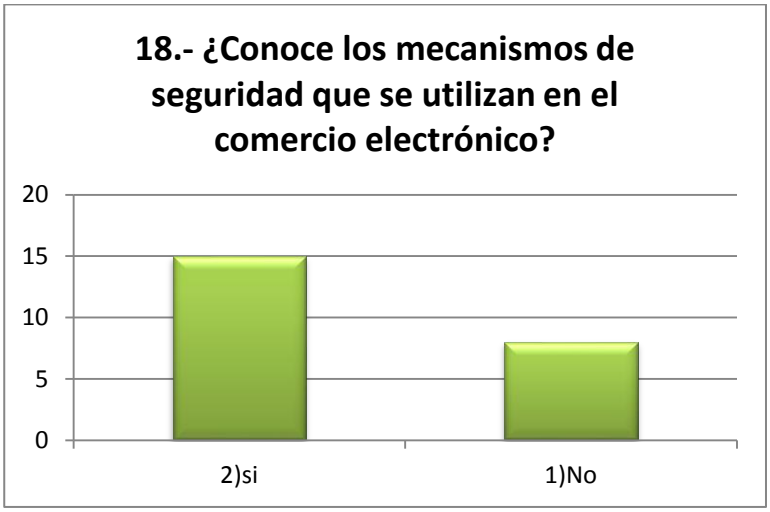


Se puede observa gráficamente, que un 69% de los usuarios encuestados les preocupa que se maneje mucha seguridad a la hora de hacer transacciones por internet, y un 22% es poca su preocupación sobre la seguridad.

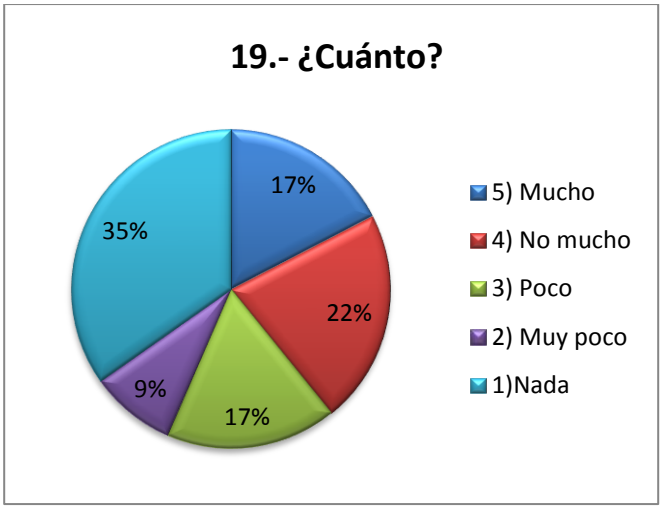
Gráficamente, se observa que, al 57% de los usuarios cuando entran a un sitio web, le toman importancia a la seguridad del sitio web, y un 30% no es mucha la importancia la que le toman.



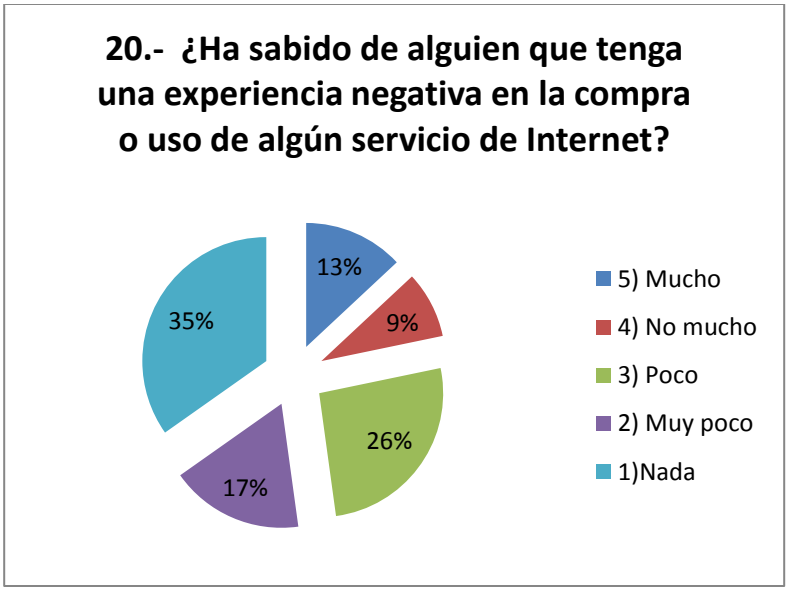
Se puede observar gráficamente, que el 70% de los usuarios, les preocupa mucho la inseguridad que existe dentro del medio de internet, y a un 6% no es mucha a la importancia que les dan la inseguridad dentro de internet..



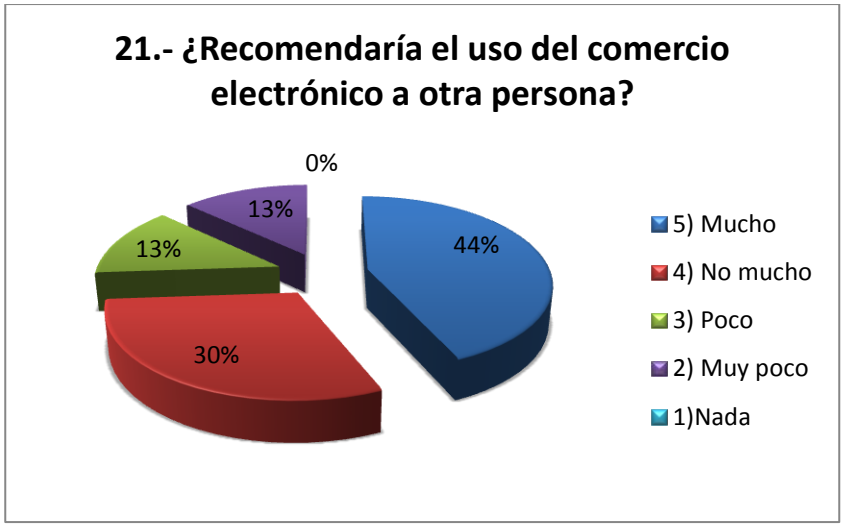
Se observa, que de las 23 personas encuestadas, 15 opinaron que si conocen los mecanismos de seguridad que se utilizan en el comercio electrónico, y solo 5 su opinión fue que no conocen dichos mecanismos.



Relacionada con la pregunta anterior, se puede observar dentro de la gráfica, que un 35% de los usuarios encuestados no conocen sobre los mecanismos de seguridad que se usan dentro del internet para el comercio electrónico, y un 17% sabes algo sobre dichos mecanismos de seguridad. Y un 22% no es mucho sus conocimientos.



Se puede observar gráficamente que un 35% de los usuarios encuestados no han sabido sobre experiencias negativas en compras por internet, un 26% poco y un 17% muy pocas experiencias conocen.



Se puede observar gráficamente que el 44% de los usuarios recomendaría el uso del comercio electrónico, el 30% de ellos no lo recomendaría mucho. Dentro de las opiniones de los usuarios, no dieron opiniones negativas sobre el comercio electrónico.

El presente cuestionario (Anexo 4. Cuestionario del la encuesta), fue aplicado por Margarita Madrigal Cruz, a las personas adultas y jóvenes de la ciudad de Las Choapas, Veracruz y Coatzacoalcos, Veracruz. En lugares como, ciber´s café, empresas y escuelas, el día 08 de julio de 2010. En este aparatado se presentan todos los resultados obtenidos en la aplicación de la encuesta.

Cuestionario codificado

1.- ¿En la actualidad hace usted uso del medio internet?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

2.- ¿Sabía usted, que por medio de internet existe el medio del comercio electrónico?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

3.- ¿Considera al Internet como un medio de comercialización, Principalmente Cómo?

5= Una moda
4= Una herramienta de compra-venta
3= Medio de difusión de productos (Mercadotecnia)
2= Medio de entretenimiento
1= otra

4.- ¿Ha realizado consultas a productos y/o servicios que involucren transacciones de comercio electrónico (compras, remates, transacciones)?

2= Si
1= No

5.- ¿Cuánto?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

6.- ¿Cuál es su grado de aceptación del comercio electrónico para usted?

5= 100%
4= 75%
3= 50%
2= 25%
1= 0%

7- ¿Ha realizado al menos una vez, alguna transacción por internet (Comprar, vender, pagos de tarjetas, consultas páginas de bancos, transacciones con tarjetas, etc.)?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

8.- ¿Cada cuanto, realiza transacciones por internet?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

9.- ¿La calidad del producto y los días de entrega, cumplieron con lo especificado en la página de dicha compra?

5= Muy alta calidad
4= Alta calidad
3= Neutra calidad
2= Baja calidad
1= Muy Baja calidad

10.- ¿Considera que los productos que se venden por medio de internet son de buena calidad y de buen costo?

5= Muy alta
4= Alta
3= Neutra
2= Baja
1= Muy Baja

11.- ¿Tuvo algún inconveniente en la página a la hora de realizar la compra?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada
¿Cuál?_____

12.- ¿La página que usted consulta para realizar una compra que tanta confianza le brinda?

5= Muy alta
4= Alta
3= Neutra
2= Baja
1= Muy Baja

13.- ¿Conoce las formas de pagos que se existen atreves de la red?

2= Si

1= No

14.- ¿Cuánto?

5= Muy alta
4= Alta
3= Neutra
2= Baja
1= Muy Baja

15.- ¿Le preocupa la seguridad en las transacciones por internet?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

16.- ¿Cuándo entra en algún sitio web, le toma importancia a la seguridad de dicho sitio?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

17.- ¿Le preocupa la inseguridad que existe en el medio de internet?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

18.- ¿Conoce los mecanismos de seguridad que se utilizan en el comercio electrónico?
2) Si

1) No

19.- ¿Cuánto?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada
20.- ¿Ha sabido de alguien que tenga una experiencia negativa en la compra o uso de algún servicio de Internet?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada
21.- ¿Recomendaría el uso del comercio electrónico a otra persona?

5=Mucho
4= No mucho
3= Poco
2= Muy poco
1= Nada

En el apartado de anexos, (Anexo 5. Codificación de la encuesta realizada. Pág.133) se encuentra la codificación de la encuesta realizada en la Ciudad de Las Choapas, Ver. y Coatzacoalcos, Ver.

4.3 PRESENTACIÓN DE LA INFORMACIÓN

La información se puede representar de muchas maneras. En este capítulo la información recolectada por medio de encuestas, esta representada, por medio de gráficas de barras y gráficas circulares.

En la presentación de la información se trata de elaborar y describir los datos de los estudios o investigaciones a través de cuadros o gráficas. El principal propósito de la etapa de presentación es facilitar la comprensión rápida y práctica de la información recién contada. Esta información se tabulará, con el fin de obtener un porcentaje por cada una de las preguntas realizadas, también se realizaran comparaciones entre ambos porcentajes, que facilitará la revisión visual rápida de las características esenciales de los datos.

Como resultado de todo este proceso se elaborarán gráficas, las que presentaran la información analizada.

CAPÍTULO V

CONCLUSIONES
Y
RECOMENDACIONES

5.1. CONCLUSIÓN DEL ESTUDIO

La fronteras nacionales será líneas dibujadas en los mapas, mientras que el flujo de negocios y el comercio correrá libremente en una economía digitalizada de sin fronteras (John Naisbitt)

La presente investigación ha sido realizada con el objetivo principal de analizar la inseguridad que se encuentra dentro de la red, y con el fin de que los usuarios puedan comprender de mejor manera como es que se maneja la seguridad dentro de los sitios web. Como todos sabemos Internet se convirtió en una valiosa herramienta para que proveedores de bienes y servicios, comerciantes, productores, y demás empresas con fines comerciales, pudieran llegar de manera directa a sus consumidores potenciales, sin importar la distancia y el tiempo, puesto que estos podrán tener acceso de desde cualquier parte del mundo y a cualquier hora del día a la información general de la compañía, el catalogo de productos, precios, ofertas, promociones, entre otros aspectos que son importantes a la hora de conquistar y ganar compradores.

La confianza es el eje y el cimiento del comercio electrónico, la cual se adquiere implementando mecanismos de seguridad óptimos. En la medida que aumenta la confianza aumenta el comercio por la redes de comunicación. Así, las actuales herramientas de seguridad deben ser utilizadas por los organismos de control y por las entidades públicas y privadas que presentan servicios públicos, así como por los empresarios. Así mismo, la asunción clara de responsabilidades por parte de los prestadores de servicios generará confianza.

A partir del intercambio de opiniones con usuarios, analistas y responsables de seguridad de infraestructura concluimos en que la tecnología de aseguramiento existe y se conoce, que las soluciones están al alcance de la mano pero que muchas empresas no desean pagar la seguridad ya que no es algo tangible.

Se ha dicho que la seguridad en la Web es difícilmente absoluta, pero se puede minimizar el riesgo utilizando medidas de seguridad apropiadas y planes para una

recuperación rápida ante un incidente de seguridad. La seguridad Web no es fácil ni barata pero la inseguridad puede ser aún más costosa. Esta debe ser parte integral de una organización y de la mentalidad de sus componentes. Poner cuidado en el desarrollo de las políticas de seguridad, posibilita evitar muchos problemas potenciales.

La seguridad del sistema de transacción de datos no debe ser un agregado al comercio electrónico, sino algo que surja desde el propio diseño.
Durante el desarrollo de la presente tesis se realizó un relevamiento de la utilización de las tecnologías del comercio electrónico en el mercado y se observó las medidas de seguridad aplicadas. Se presentaron los conceptos que permiten al usuario detectar sitios seguros y confiar en ellos; se analizaron las técnicas existentes de certificación de sitios seguros y los mecanismos de certificación y seguridad para encontrar las formas de persuasión que, basadas en la tecnología, le permitan a las empresas que sus clientes confíen en dichas transacciones.
También se comentaron las diferentes herramientas de protección, las prácticas y arquitecturas que aumentan la seguridad. Las técnicas de identificación digital mediante certificados, protocolos y sellos de confianza.

Utilizando medidas de seguridad, buenas prácticas y arquitecturas que pueden asegurar al cliente la integridad y fiabilidad de sus datos se logra la tan anhelada confianza y satisfacción que es el objetivo primordial de cualquier empresa para subsistir en un mercado competitivo.

El usuario debe estar al tanto de los riesgos y cómo defenderse ya sea de las formas de prevención como de las posibilidades de reaccionar ante ataques.
Somos nosotros, los profesionales de sistemas, los que tenemos que mostrarles los peligros verdaderos y los mecanismos de defensa que existen en su favor.

El usuario mexicano está protegido cuando realiza compras por internet. La Ley Federal de Protección al Consumidor (LFPC) contiene disposiciones generales sobre comercio electrónico en su capítulo VIII (De los derechos de los

consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología).

Las empresas de venta en línea tienen que transmitir la idea de seguridad al cliente, sino simplemente huirá de su sitio. De esto dependerá el éxito o el fracaso del comercio electrónico.

Finalmente, puede afirmarse que es posible realizar el comercio electrónico gracias a las diferentes herramientas de seguridad que ofrece el mercado. El desarrollo orientado a la cobertura y a la reducción de costos. El comercio electrónico es, un mercado de futuro que poco a poco va creciendo y creando nuevas empresas que pueden ser de gran ayuda para intentar ahorrar sin tener que prescindir de buenas cosas. Una nueva forma de comprar que nos permite estar a la última y ahorrar no sólo en dinero sino en tiempo. Comprar nunca había sido tan fácil. Tal es el éxito que están adquiriendo estas empresas que incluso la principal plataforma de comercio electrónico del mundo.

5.2. SUGERENCIAS

- El impacto del que esta generando el uso de comercio electrónico y que generará es arrollador, tanto en las empresas como en la sociedad en su conjunto.
- Si el auge del comercio electrónico sigue creciendo, será necesario la creación de autoridades de registro, que posean una gran base de datos y hagan aún más seguro y confiable el sistema. Autoridades que deben ser creadas por los países, para que a través de pactos internacionales se establezcan canales de comunicación mundial, ampliando el concepto de globalización y haciendo el comercio electrónico su ejemplo más destacado.
- Las instituciones bancarias son las que han realizado mayor avance en el comercio electrónico con la implantación de las operaciones bancarias por medio de internet, preocupándose con prioridad en el tema de la seguridad y privacidad de la información, es aquí donde los usuarios deben de tener la información necesaria para saber cómo es el funcionamiento de estas implementaciones, donde las instituciones bancarias deben de exponer este tipo de información.
- Se debería de actualizar cada día la información que se maneja dentro del ámbito de la seguridad en el comercio electrónico. Exponer la información, tanto a los usuarios como a las empresas, como un tema de importancia.
- Debe forjarse el ámbito de las transacciones por medio electrónicos, normas claras y equitativas, en cuanto a la asunción de riesgos.

5.3. GLOSARIO

Acceso remoto: es una tecnología que permite a un usuario trabajar en una computadora a través de su escritorio gráfico desde otro terminal ubicado en otro lugar.

Administración de cuentas de usuarios.- es la forma a través de la cual se identifica y autentifica a un individuo con el sistema. Las cuentas de usuarios tienen diferentes componentes. Primero, esta el nombre de usuario. Luego, está la contraseña, seguida de la información de control de acceso.

Antivirus.- son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos. El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

AOL.- es una empresa de servicios de internet y medios con sede en Nueva York. Ha franquiciado sus servicios a empresas en varios países alrededor del mundo o establecido versiones internacionales de sus servicios.

Aprovisionamiento electrónico.- (en inglés, *Electronic Procurement*,) consiste en el uso de nuevas tecnologías que automatizan y optimizan la función de compras de una empresa.

ARPANET (*Advanced Research Projects Agency Network*) ARPA era enlazar diferentes ordenadores todos juntos, para mejorar la potencia general del procesamiento de los ordenadores y descentralizar el almacenamiento de información.

Autenticación.- En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.

Biométrica.- se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Blogs.- o en español también una *bitácora*, es un sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente. El nombre *bitácora* está basado

en los cuadernos de bitácora, cuadernos de viaje que se utilizaban en los barcos para relatar el desarrollo del viaje y que se guardaban en la bitácora

Certificado digital.- es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

CGI (*Common Gateway Interface*) Interfaz de entrada común**,** es una importante tecnología de la World Wide Web que permite a un cliente (navegador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el programa. Es un mecanismo de comunicación entre el servidor web y una aplicación externa cuyo resultado final de la ejecución son objetos MIME. Las aplicaciones que se ejecutan en el servidor reciben el nombre de CGIs.

Cibermediario.- puede denotar varios significados relevantes a los medios de comunicación, pero coincide en el elemento primordial: el uso del ciberespacio. Por una parte, se puede entender por cibermedio al canal o medio electrónico por el cual es transmitida la información (un Podcast, el email, la radio y televisión por Internet, entre otros).

Cifrado.- es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra a través de Internet, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo. Use el cifrado cuando desee un alto nivel de protección de la información.

Cifrado asimétrico.- es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Cifrado simétrico.- es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Criptografía.- es la técnica (bien sea aplicada al arte o la ciencia) que altera las representaciones Lingüísticas de un mensaje.

Collaborative commerce (Colaboración Comercio).- Colaboración Comercio permite a los minoristas, proveedores y distribuidores para compartir información entre sí en un idioma estándar de negocios, beneficiando a todos los miembros de la cadena de suministro. Esta iniciativa incluye los procesos, tecnologías y normas de apoyo que permiten la comunicación continua y automatizada de la información electrónica entre los socios comerciales.

Comercio electrónico.- también conocido como ***e-commerce*** (*electronic commerce* en inglés), consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos.

Conexión única "Single Sign on- SSO".- (SSO) es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

Consumidor a consumidor (C2C, CONSUMER TO CONSUMER).- Se refiere a la venta entre consumidores individuales, presenta un sitio web con una plataforma de intercambio desde la cual los consumidores finales hacen sus transacciones económicas, por ejemplo, subastas basadas en web. Este modelo consiste en ofrecer dos o más ítems para la venta con el mismo precio y en función de las reglas (mejor oferta, mejor oferente) se cierran la subasta y se ejecuta la compraventa.

Consumidor a negocio (C2B, CONSUMER TO BUSINESS).- Se define como el contrato comercial realizado a través de internet que se materializa cuando un consumidor o particular visita la dirección web de una empresa y se realiza una venta.

Cualitativa .- es un método de investigación usado principalmente en las ciencias sociales que se basa en cortes metodológicos basados en principios teóricos tales como la fenomenología, hermenéutica, la interacción social empleando métodos de recolección de datos que son no cuantitativos, con el propósito de explorar las relaciones sociales y describir la realidad tal como la experimentan los correspondientes.

Cuantitativo.- es aquella que permite examinar los datos de manera numérica, especialmente en el campo de la Estadística.

DARPA. Defense Advanced Research Projects Agency (Agencia de Investigación de Proyectos Avanzados de Defensa) es una agencia de defensa con un papel único dentro del Departamento de Defensa. DARPA no está vinculado a una misión operacional específica: DARPA proporciona opciones tecnológicas para el Departamento entero, y está diseñado para ser el motor tecnológico en la transformación del Departamento de Defensa.

Decretos ejecutivos (gobierno).- es un tipo de acto administrativo emanado habitualmente del poder ejecutivo y que, generalmente, posee un contenido normativo reglamentario, por lo que su rango es jerárquicamente inferior a las leyes

Desencriptación.- Recuperación del contenido real de una información cifrada previamente.

Detección.- es el proceso de decidir cuál de las posibles señales que puede originar una fuente es la que con mayor probabilidad generó una señal recibida.

Dinero electrónico.- (también conocido como *e-money*, *efectivo electrónico*, *moneda electrónica*, *dinero digital*, *efectivo digital* o *moneda digital*) se refiere a dinero que se intercambia sólo de forma electrónica. Típicamente, esto requiere la utilización de una red de ordenadores, la Internet y sistemas de valores digitalmente almacenados.

Eavesdropping.- termino inglés que traducido al español significa *escuchar secretamente*, se ha utilizado tradicionalmente en ámbitos relacionados con la seguridad, como escuchas telefónicas.

EDI.- son las siglas de *Electronic Data Interchange*, intercambio electrónico de datos. El sistema EDI permite el intercambio (envío y recepción) de documentos comerciales por vía telemática.

EDS (Electronic Data Systems).- es una empresa estadounidense de consultoría de tecnologías de la información que definió al negocio "outsourcing" cuando se fundó en 1962 por Ross Perot.

Encriptación.- es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

EPS (Sistemas de Pagos Electrónicos).- realiza la transferencia del dinero entre comprador y vendedor en una compra-venta electrónica. Es, por ello, una pieza fundamental en el proceso de compra-venta dentro del comercio electrónico.

Exchange to Exchange (E2E). En Internet, E2E se ha utilizado en el sentido de cambio de tipo de cambio - es decir, el intercambio de información o transacciones entre los sitios Web que se sirven como intercambio o corredores de bienes y servicios entre empresas.

Extranet.- Es una red privada que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización.

Facilidad.- Condiciones o circunstancias que permiten conseguir o realizar algo, especialmente el pago de un producto o un servicio.

Firewall (Cortafuegos).- es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Firma digital.- es una firma electrónica que puede ser utilizada para autenticar la identidad de quien envía un mensaje o quien firma un documento, y hace posible garantizar que el contenido original de un mensaje o documento ha sido enviado sin modificaciones.

Fraudes telefónicos.- es un delito. Los delincuentes usan el teléfono para cometer varios tipos diferentes de fraude, entre los que se incluyen los fraudes de sorteos y loterías, fraudes con préstamos, membrecías de clubes de compras y estafas de tarjetas de crédito.

G7/G8.- es un grupo de países formado en 1999 por los siete países más industrializados (G-7), Rusia (G-7+1 o G-8), once países recientemente industrializados de todas las regiones del mundo, y la Unión Europea como bloque.

Gobierno a ciudadanos (G2C, GOVERNMENT TO CITIZENS).- es el enlace de comunicación entre un gobierno y los particulares o de residentes. Dicha comunicación G2C mayoría de las veces se refiere a lo que se lleva a cabo a través de Tecnologías de la Información Comunicación (TIC), pero también puede incluir la publicidad directa y las campañas de los medios de comunicación. G2C puede tener lugar en el gobierno federal, estatal y local.

Handshake Protocol.- Es uno de los posibles protocolos que pueden encapsularse sobre la capa anterior y permite al cliente y al servidor autenticarse mutuamente, negociar un algoritmo de cifrado e intercambiar llaves de acceso. Una de las ventajas del SSL es que es independiente del protocolo de aplicación, ya que es posible ubicarlo por encima del mismo en forma transparente.

Hardware.- corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Http- Hypertext Transfer Protocol o **HTTP** (*protocolo de transferencia de hipertexto*) es el protocolo usado en cada transacción de la World Wide Web. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo

orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

Https- Hypertext Transfer Protocol Secure (Protocolo *seguro de transferencia de hipertexto*), más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

IIS (Internet Information Server).- es un conjunto de servicios para servidores usando Microsoft Windows. Es especialmente usado en servidores web, que actualmente es el segundo más popular sistema de servidor web.

Infraestructura de clave pública.- (o, en inglés, PKI, *Public Key Infrastructure*) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Informática Forense.- es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Intercambio electrónico de Datos "EDI".- (*Electronic Data Interchange***)** permite el intercambio (envío y recepción) de documentos comerciales por vía telemática. Albaranes, facturas, órdenes de compra y otros documentos comerciales electrónicos pueden tramitarse directamente desde el ordenador de la empresa emisora al de la empresa receptora, con gran ahorro de tiempo y evitando muchos errores, propios de la comunicación tradicional “en papel”.

Intangibilidad.- es un adjetivo que califica todo aquello que no tiene una presencia física, lo que no puede -o debe- ser tocado jamás.

Integridad.- es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información.

Internet.- es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las

redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

Intrabusiness (ORGANIZACIONAL, EC).- actividades del comercio electrónico realizado dentro de una organización, entre una empresa y sus empleados, entre las unidades dentro de la empresa, entre los empleados en el mismo negocio, Empresa a los empleados, intrabusiness en que una organización ofrece productos o servicios a sus empleados.

IP- seguridad IP (IPSec, Internet Protocol security).- es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

ISP (proveedor de servicios de Internet).- es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cablemódem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, servidores de noticias, entre otras.

Llave privada.- es almacenada sólo en su computadora a través de su navegador Web. Usted nunca debería copiar o enviar su llave privada a otra persona. Dependiendo de navegador Web que use y su configuración de seguridad, usted podría tener una contraseña asociada con su llave privada. Esto es protección adicional para usted, de tal forma que si alguien consigue su llave privada o usa su computadora, no puede usar la llave privada (o su Certificado Digital).

Man-in-the-middle (*intermediario*).- es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

Malware.- también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

Marketing.- es la orientación con la que se administra el mercadeo o la comercialización dentro de una organización.

Metamediarios (subastas).- es una venta organizada de un producto basado en la competencia directa, y generalmente pública, es decir, a aquel comprador (postor) que pague la mayor cantidad de dinero o de bienes a cambio del producto.

Microprocesador.- es el circuito integrado más importante, de tal modo, que se le considera el cerebro de una computadora. Está constituido por millones de transistores integrados.

Mobile commerce (comercio móvil).- es una transacción que implica la transferencia de la propiedad o derechos de uso de bienes y servicios, que se ha iniciado y/o completado mediante el acceso móvil a redes mediana-ordenador con la ayuda de un dispositivo electrónico.

Negocio a consumidor (B2C, BUSINESS TO CONSUMER).- Forma de comercio electrónico en donde las operaciones comerciales son entre una empresa y un usuario final.

Negocio a empleado (B2E, BUSINESS TO EMPLOYES).- es la relación comercial que se establece entre una empresa y sus propios empleados. Por ejemplo, una empresa aérea puede ofrecer paquetes turísticos a sus empleados a través de su propia intranet y, además de sus ofertas puede incluir las de compañías aéreas asociadas.

Negocio a negocio (B2B, B2B, BUSINESS TO BUSINESS).-Forma de comercio electrónico en donde las operaciones comerciales son entre empresas y no con usuarios finales.

No repudio.- es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

NSF (National Science Foundation).- es una agencia del gobierno de Estados Unidos independiente que impulsa investigación y educación fundamental en todos los campos no médicos de la Ciencia y la Ingeniería.

NSFnet.- National **S**cience **F**oundation's **Net**work.

Ordenadores (*un computador*).- es una máquina electrónica que recibe y procesa datos para convertirlos en información útil.

Pago electrónica.- es definido como cualquier operación de pago realizada con una tarjeta de pista magnética o con un microprocesador incorporado, en un grupo terminal de pago electrónico o terminal de punto de venta**.**

Persona a persona (P2P PEOPLE TO PEOPLE). - Relación directa entre dos personas.

PGP (Pretty Good Privacy, *privacidad bastante buena***).-** es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

Phishing.- es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Post-venta.- Consiste en todos aquellos esfuerzos después de la venta para satisfacer al cliente y, si es posible, asegurar una compra regular o repetida.

Prevención de intrusos.- es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Pre-venta.- se puede definir como la atención al cliente antes de la venta, en el sentido del conocimiento de sus necesidades y características.

Protocolo de control de transacción (TCP).- es uno de los protocolos fundamentales en Internet. Es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte.

Protocolo SET (Transacción electrónica segura).- es un protocolo estándar para proporcionar seguridad a una transacción con tarjeta de crédito en redes de computadoras inseguras, en especial Internet.

Puja.- El precio más alto que el comprador está ofreciendo para una determinada divisa en ese momento; la diferencia entre el precio de *puja,* o precio de demanda, es el "spread" o margen.

PYMES (pequeñas y medianas empresas).- son empresas con características distintivas, y tienen dimensiones con ciertos límites ocupacionales y financieros prefijados por los Estados o Regiones. Son agentes con lógicas, culturas, intereses y un espíritu emprendedor específicos. Usualmente se ha visto también el término MIPyMEs (acrónimo de "micro, pequeñas y medianas empresas"), que es una expansión del término original, en donde se incluye a la microempresa.

Recuperación de datos.- es el proceso mediante el cual se trata de recuperar el contenido de un dispositivo de almacenamiento de datos informático que se encuentra dañado, estropeado o inaccesible de forma normal.

Redes piramidales (Marketing multinivel).- es un negocio ilegal* (en USA) de producción de dinero. El nombre se le da porque su estructura tiene la forma de una pirámide. En un esquema piramidal típico, unos pocos participantes que están en la parte superior reclutan nuevos participantes para la parte inferior. Estos nuevos participantes pagan dinero para entrar al esquema y deben reclutar participantes adicionales para mantener la pirámide funcionando. En un esquema

piramidal simplemente circula dinero entre los participantes. No se consigue dinero adicional.

Riesgos.- Cuanto mayor es la vulnerabilidad mayor es el riesgo (e inversamente), pero cuanto más factible es el perjuicio o daño mayor es el peligro (e inversamente). Por tanto, el riesgo se refiere sólo a la teórica "posibilidad de daño" bajo determinadas circunstancias, mientras que el peligro se refiere sólo a la teórica "probabilidad de accidente o patología" bajo determinadas circunstancias, sucesos que son causas directas de daño.

Redes Virtuales Privadas "VPNs".- es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo.

Seguridad.- proviene de la palabra securitas del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

Seguridad de la capa de transporte (TLS, Transport Layer Security).- es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor. Así el intercambio de información se realiza en un entorno seguro y libre de ataques.

SET (Transacción electrónica segura).- es un protocolo estándar para proporcionar seguridad a una transacción con tarjeta de crédito en redes de computadoras inseguras, en especial Internet.

Software.- es el equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Spyware (programa espía).- es un programa, dentro de la categoría malware, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

SSH (Secure Shell, intérprete de órdenes segura**).-** es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SSL (Secure Socket Layer).- Protocolo de Capa de Conexión Segura, son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet. Proporciona autenticación y privacidad de la información

entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI).

TCP/IP.- es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

Transferencia Electrónica de Fondos "EFT".- servicios bancarios. Este servicio permite a los usuarios y cuenta habientes poder realizar transacciones de transferencias de fondos de una cuenta de un banco a una cuenta en otro banco.

Transacción.- es una actividad que consiste en entregar una cosa para recibir otra a cambio. Pero conviene subrayar que esa definición de transacción puede ser entendida en un sentido muy amplio.

TPV-V (Terminal Punto de Venta Virtual).- Hace referencia al dispositivo y tecnologías que ayudan en la tareas de gestión de un establecimiento comercial de venta al público. También a los sistemas que bancos o cajas de ahorros utilizan para que transacciones a través de Internet sean seguras, normalmente en tiendas "on line".

UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT).- es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que estudia los aspectos técnicos, de explotación y tarifarios y publica normativa sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial.

URL (localizador uniforme de recursos).- es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, videos, presentaciones digitales, entre otras.

Voto electrónico.- es una expresión que comprende varios tipos de votación, que abarca tanto modos electrónicos de emitir votos como medios electrónicos de contar los votos. Las tecnologías para el voto electrónico pueden incluir tarjetas perforadas, sistemas de votación mediante escáneres ópticos y quioscos de votación especializados (incluso sistemas de votación auto contenidos.

Web.- que es un conjunto de páginas web, típicamente comunes a un dominio o subdominio en la World Wide Web.

World Wide Web.- (literalmente telaraña de alcance mundial), cuya traducción podría ser *Red Global Mundial* o "Red de Amplitud Mundial", es un sistema de documentos de hipertexto o hipermedios enlazados y accesibles a través de Internet. Con un navegador web, un usuario visualiza sitios web compuestos de

páginas web que pueden contener texto, imágenes, videos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

X.509.- es un estándar UIT-T para infraestructuras de claves públicas (en inglés, *Public Key Infrastructure* o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

BIBLIOGRAFÍA

1. Alonso Conde Ana Bellén. Comercio electrónico: Antecedentes y estado actual. 2004. Editorial Dukinson. Madrid. Pág. 96.

2. Alberto León García, Indira Widjaja. Redes de comunicación. Conceptos fundamentales y arquitectura básicas. 2002. Editorial Mc-Graw-Hill. Primera edición en español. España. Pág. 771.

3. Aspatore R. Jonathan. Traducido por Rojas Martínez Iván. Al día en el comercio electrónico. 2001. Editorial Mac Graw-Hill. México. Pág. 182

4. Brambila Ibáñez Berenice. Manual para la elaboración de tesis. 2007. Editorial Trillas. México. Pág. 303.

5. Cohen Daniel, Asim Enrique. Sistemas de información para los negocios. 2000. Editorial Mc Graw-Hill/interoamericana. Tercera edición. México. Pág. 413

6. Cohen Daniel, Asim Enrique. Sistemas de información para los negocios. 2005. Editorial Mc Graw-Hill/interoamericana. Cuarta edición. México. Pág. 346

7. De Águila Rosa Ana. Comercio electrónico y estrategia empresarial. Hacia la economía digital. . Editorial Alfa-omega Rama. Segunda edición. Pág. 194

8. De Núñez Alberto Fernando, Lugones. Modelos de negocios en internet. 2001. Editorial Mc Graw-Hill/profesional. Tomo II. España. Pág. 365

9. Estallo de los A. María. Empresa virtual de la idea a la acción. 2001. Editorial Esic. España. Pág. 311.

10. Garballar A. José. Internet. Libro de navegamiento. 2000. Editorial Rama. Segunda edición. Pág. 482

11. Hernández Cázares Laura, Christen María, Levi Jaramillo Enrique, Roca Villaseñor Leticia. Técnicas actuales de investigación documental. 2007. Editorial Trillas. México. Pág. 194.

12. Julián Briz/ Isidro Laso. Internet y comercio electrónico. 2001. Editorial Granica. México. Pág. 537

13. M. Siebel Thomas. Principios del E-Business. 2001. Editorial Granica. Barcelona. Pág. 338.

14. Haig Matt. Traducido por Brava J.A. Fundamentos del Comercio Electrónico. 2001. Editorial Matt Hing. Primera edición. España Pág. 158.

15. Nash Andrew, Duane William, Joseph Celia, Brink Derek. Traducido por De Barón Ávila Cecilia. PIK Infraestructura de claves públicas. La mejor tecnología para implementar y administrar la seguridad de su negocio. 2002. Editorial Mc Graw-Hill. Primera edición. Colombia. Pág. 512

16. López Islas Noé. Comercio electrónico. Centro de computación propuesto en México. 2001. Editorial Mc Graw-Hill. México. Pág. 116

17. Lozano Medina Luis. Métodos de investigación I y II. Emma E. Paniagua Roldan. 2004. México. Pág. 32

18. Nombela José Juan. Seguridad informática. . Editorial Parainfo. Edición . España. Pág. 257

19. Oelkers Boen Dotty. Comercio electrónico. 2004. Editorial Thompson. Series Business. México. Pág. 168

20. Rodao Marcelo de Jesús. Piratas Cibernéticos. Cyberwars, seguridad de la información e internet. 2001. Editorial Rama. Pág. 247

21. Sampieri Hernández Roberto. Metodología de la investigación. 2007. Editorial Mc Graw-Hill. Cuarta edición. México. Pág. 850

22. Seoane Balado Eloy. La nueva era del comercio: comercio electrónico. Editorial Vigo. 2005. 1 edición. España. Pág. 302

23. Soriano Rojas Raúl. Guía para realizar investigaciones sociales. 1994. Editorial Plaza y valdes. Catorceava edición. México. Pág. 286

24. Soriano Rojas Raúl. El proceso de la investigación científica. 2005. Editorial trillas. México. Pág. 150

25. Turban Efraim. Electronic Commerce 2002. 2002. New Jersey. Pág. 914

Referencias Bibliográficas

De Águila Rosa Ana. Comercio electrónico y estrategia empresarial. Pág. 61

[2] Seoane Balado Eloy. La nueva era de comercio: el comercio electrónico. Pág. 9

[3] Seoane Balado Eloy. La nueva era de comercio: el comercio electrónico. Pág. 10

[4] Seoane Balado Eloy. La nueva era de comercio: el comercio electrónico. Pág. 11

[5] Seoane Balado Eloy. La nueva era de comercio: el comercio electrónico. Pág. 13

[6] De Núñez Alberto Fernando, Lugones. Modelos de negocios en internet. pág.46

[7] Seoane Balado Eloy. La nueva era del comercio: comercio electrónico. Pág. 4.

[8] M. Siebel Thomas. Principios del E-Business. Pág. 13

[9] Seoane Balado Eloy. La nueva era del comercio: comercio electrónico. Pág. 4.

[10] Oelkers Boen Dotty. Comercio electrónico.. Series Business. Pág. 32

[11] Oelkers Boen Dotty. Comercio electrónico.. Series Business. Pág. 33

[12] Turban Efraim. Electronic Commerce. 2002. Pág. 432

[13] Cohen Daniel, Asim Enrique. Sistemas de información para los negocios. Pág. 243

[14] Cohen Daniel, Asim Enrique. Sistemas de información para los negocios. Pág. 245

[15] Cohen Daniel, Asim Enrique. Sistemas de información para los negocios. Pág. 247

[16] De Núñez Alberto Fernando, Lugones. Modelos de negocios en internet. Pág. 49

[17] http://www.ahorrando.org/Templates/ah/Content.aspx?id=782

[18] De Núñez Alberto Fernando, Lugones. Modelos de negocios en internet. Pág. 52

[20] ISACA (2008). *ISACA MANUAL DE PREPARACIÓN AL EXAMEN CISM 2008*. Information Systems Audit and Control Association.. Pág-. 17

[22] Turban Efraim. Electronic Commerce 2002. 2002. New Jersey. Pág. 914

[23] Alberto León García. Redes de Comunicación. Conceptos Fundamentales y Arquitectura Básicas. pág. 4

[24]Turban Efraim. Electronic Commerce 2002. 2002. New Jersey. Pág. 356

[26]Alberto León García, Indira Widjaja. Redes de comunicación. Conceptos fundamentales y arquitectura básicas. 2002. Pág. 4.

[2]9Nash Andrew, Duane William. Joseph Celia, Brink Derek. PIK Infraestructura de claves públicas. La mejor para implementar y administrar la seguridad de su negocio tecnología. Pág. 44

[30] Turban Efraim. Electronic Commerce 2002. 2002. New Jersey. Pág. 378

[31] Turban Efraim. Electronic Commerce 2002. 2002. New Jersey. Pág. 385

[33] Nombela José Juan. Seguridad informática. Pág. 232

[34]Nash Andrew, Duane William, PIK Infraestructura de claves públicas. Pág. 17

[35] Nash Andrew, Duane William, PIK Infraestructura de claves públicas. Pág. 41

[36] Sampieri Hernández Roberto. Metodología de la investigación. 2007. Pág. 91.

Referencias de medios electrónicos

[19]http://www.wikilearning.com/curso_gratis/la_seguridad_en_informatica-comercio_electronico/3625-9

[21] http://www.maestrosdelweb.com/editorial/segecom/

[25] The SSL Protocol, V 3.0, http://wp.netscape.com/eng/ssl3/draft302.txt

[27] La definición del protocolo HTTP, documento que puede ser localizado en la dirección: http://www.faqs.org/rfcs/rfc2616.html

[28] http://www.faqs.org/rfcs/rfc4252.html

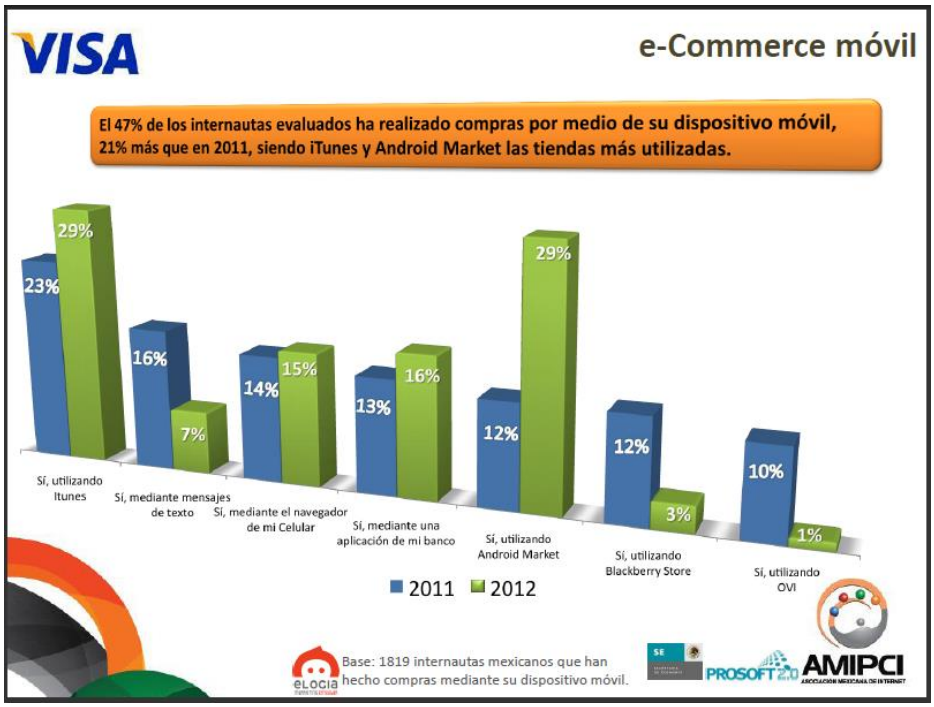
[32] http://www.maestrosdelweb.com/editorial/segecom/

[33]http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm

A N E X O S

Anexo1. Gráfica A. Razones para no comprar en internet. Estudio por AMIPCI

Anexo 2. Grafica B E-Commerce móvil



Anexo 3.- Phishing

Phishing (suplantación de identidad) es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Los intentos más recientes de phishing han tomado como objetivo a clientes de bancos y servicios de pago en línea. En términos generales, esta variante hacia objetivos específicos en el phishing se ha denominado spear phishing (literalmente pesca con arpón). Los sitios de Internet con fines sociales también se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad. Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques phishing en redes sociales.

Técnicas de phishing

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar el impostor. URLs mal escritas o el uso de subdominios son trucos comúnmente usados por phishers, como el ejemplo en esta URL, http://www.nombredetubanco.com.ejemplo.com/. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares). Por ejemplo, el enlace http://www.google.com@members.tripod.com/ puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente). Este método ha sido erradicado desde entonces en los navegadores de Mozilla e Internet Explorer. Otros intentos de phishing utilizan comandos en JavaScripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

En otro método popular de phishing, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como Cross Site Scripting) los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Hay varios programas informáticos anti-phishing disponibles. La mayoría de estos programas trabajan identificando contenidos phishing en sitios web y correos electrónicos; algunos software anti-phishing pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el phishing recibidos por el usuario.

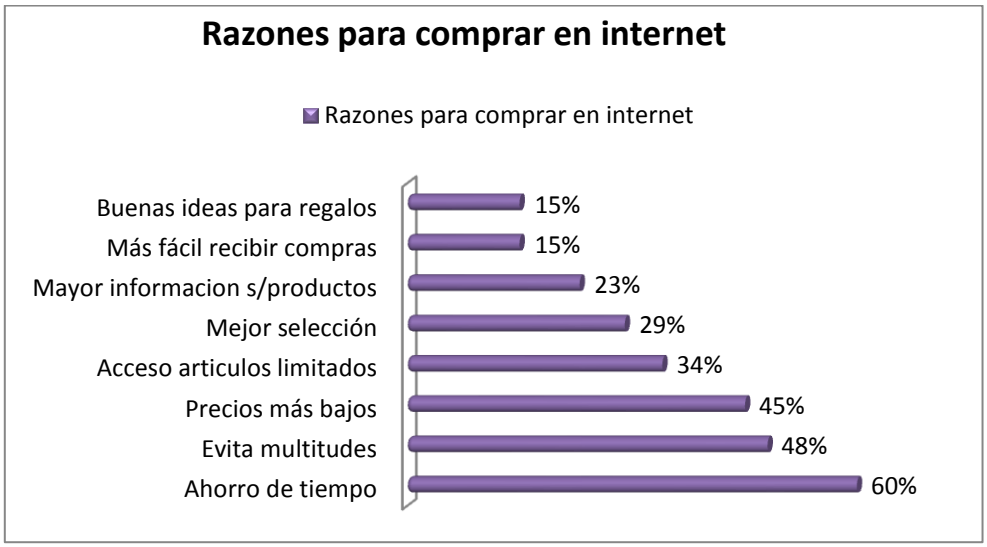
Medidas de prevención para evitar ser víctima del “phishing”

Las siguientes medidas buscan asistirlo para minimizar los efectos negativos de un ataque de “phishing” y de ser posible, impedirlo:

- **Si recibe un correo electrónico que le pide información personal o financiera, no responda. Si el mensaje lo invita a acceder a un sitio web a través de un enlace incluido en su contenido, no lo haga.** Las organizaciones que trabajan seriamente están al tanto de este tipo de fraudes y por consiguiente, no solicitan información por medio del correo electrónico. Tampoco lo contactan telefónicamente, ni mediante mensajes SMS o por fax. Si le preocupa el estado de la cuenta que posee en la organización que dice haber enviado el correo, o que lo ha contactado, comuníquese directamente utilizando un número telefónico conocido y provisto por la entidad u obtenido a través de medios confiables, como por ejemplo de su último resumen de cuenta. Alternativamente, puede ingresar en la página oficial de la organización, ingresando usted mismo la dirección de Internet correspondiente en el navegador.
- **No envíe información personal usando mensajes de correo electrónico.** El correo electrónico, si no se utilizan técnicas de cifrado y/o firma digital, no es un medio seguro para enviar información personal o confidencial.

- **No acceda desde lugares públicos.** En la medida de lo posible, evite ingresar al sitio web de una entidad financiera o de comercio electrónico desde un cyber-café, locutorio u otro lugar público. Las computadoras instaladas en estos lugares podrían contener software o hardware malicioso destinado a capturar sus datos personales.
- **Verifique los indicadores de seguridad del sitio web en el cuál ingresará información personal.** Si es indispensable realizar un trámite o proveer información personal a una organización por medio de su sitio web, escriba la dirección web usted mismo en el navegador y busque los indicadores de seguridad del sitio. Al acceder al sitio web, usted deberá notar que la dirección web comienza con “https://”, donde la “s” indica que la transmisión de información es “segura”. Verifique también que en la parte inferior de su navegador aparezca un candado cerrado. Haciendo clic sobre ese candado, podrá comprobar la validez del certificado digital y obtener información sobre la identidad del sitio web al que está accediendo.
- **Mantenga actualizado el software de su PC:** Instale las actualizaciones de seguridad de su sistema operativo y de todas las aplicaciones que utiliza, especialmente las de su producto antivirus, su cliente web y de correo electrónico. La mayoría de los sistemas actuales permiten configurar estas actualizaciones en forma automática.
- **Revise sus resúmenes bancarios y de tarjeta de crédito tan pronto los reciba.** Si detecta cargos u operaciones no autorizadas, comuníquese de inmediato con la organización emisora. También contáctese con ella si se produce una demora inusual en la recepción del resumen.
- **No descargue ni abra archivos de fuentes no confiables.** Estos archivos pueden tener virus o software malicioso que podrían permitir a un atacante acceder a su computadora y por lo tanto, a toda la información que almacene o introduzca en ésta.

RAZONES PARA COMPRAR EN INTERNET



Gráfica 1.1.- Razones para comprar en internet

Esta gráfica nos muestra un porcentaje de las razones para comprar en internet, según el informe Índice de Compras VIII-Greendield-IT 2012 en la cual las respuestas de los usuarios son sumamente coherentes con las expectativas, ya que perciben fácilmente las ventajas de las compras en línea: comodidad, variedad e información. Los precios también son uno de los factores determinantes en las preferencias de los usuarios.

Anexo 4.- Cuestionario

ENCUESTA SOBRE EL COMERCIO ELECTRONIO

Edad:_____ Fecha: _____

Ocupación: _____

Bueno día, se está realizando una encuesta para evaluar el manejo del comercio electrónico, en la ciudadanía. Le agradeceremos brindarnos un minuto de su tiempo para responder las siguientes preguntas. Subraya tu respuesta.

1.- ¿En la actualidad hace usted uso del medio internet?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

2.- ¿Sabía usted, que por medio de internet existe el medio del comercio electrónico?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

3.- ¿Considera al Internet como un medio de comercialización, Principalmente Cómo?

5) Una moda 4) Una herramienta de compra-venta 3) Medio de difusión de productos (Mercadotecnia)

2) Medio de entretenimiento 1) otra_____

4.- ¿Ha realizado consultas a productos y/o servicios que involucren transacciones de comercio electrónico (compras, remates, transacciones)?

2) Si 1) No

5.- ¿Cuánto?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

6.- ¿Cuál es su grado de aceptación del comercio electrónico para usted?

5) 100% 4) 75% 3) 50% 2) 25% 1) 0%

7- ¿Ha realizado al menos una vez, alguna transacción por internet (Comprar, vender, pagos de tarjetas, consultas páginas de bancos, transacciones con tarjetas, etc.)?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

8.- ¿Cada cuanto, realiza transacciones por internet?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

9.- ¿La calidad del producto y los días de entrega, cumplieron con lo especificado en la página de dicha compra?

5) Muy alta 4) Alta 3) Neutra 2) Baja 1) Muy Baja

10.- ¿Considera que los productos que se venden por medio de internet son de buena calidad y de buen costo?

5) Muy alta 4) Alta 3) Neutra 2) Baja 1) Muy Baja

11.- ¿Tuvo algún inconveniente en la página a la hora de realizar la compra?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

¿Cuál?_____

12.- ¿La página que usted consulta para realizar una compra que tanta confianza le brinda?

5) Muy alta 4) Alta 3) Neutra 2) Baja 1) Muy Baja

13.- ¿Conoce las formas de pagos que se existen atreves de la red?

2) Si 1) No

14.- ¿Cuánto?

5) Muy alta 4) Alta 3) Neutra 2) Baja 1) Muy Baja

15.- ¿Le preocupa la seguridad en las transacciones por internet?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

16.- ¿Cuándo entra en algún sitio web, le toma importancia a la seguridad de dicho sitio?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

17.- ¿Le preocupa la inseguridad que existe en el medio de internet?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

18.- ¿Conoce los mecanismos de seguridad que se utilizan en el comercio electrónico?

2) Si 1) No

19.- ¿Cuánto?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

20.- ¿Ha sabido de alguien que tenga una experiencia negativa en la compra o uso de algún servicio de Internet?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

21.- ¿Recomendaría el uso del comercio electrónico a otra persona?

5) Mucho 4) No mucho 3) Poco 2) Muy poco 1) Nada

Anexo5. Codificación de los resultados.

	NUMERO DE PERSONAS ENCUESTADAS																							
PREGUNTAS	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**TOTAL**
1	*5*	*5*	*5*	*3*	*5*	*5*	*5*	*3*	*5*	*5*	*5*	*5*	*3*	*5*	*5*	*4*	*5*	*5*	*5*	*5*	*4*	*5*	*5*	107
2	*4*	*5*	*5*	*5*	*3*	*5*	*4*	*5*	*3*	*5*	*5*	*5*	*4*	*5*	*5*	*5*	*5*	*4*	*5*	*5*	*5*	*5*	*5*	107
3	*4*	*3*	*4*	*2*	*1*	*3*	*4*	*4*	*1*	*4*	*3*	*1*	*4*	*4*	*1*	*4*	*2*	*3*	*4*	*4*	*4*	*1*	*1*	66
4	*2*	*2*	*2*	*2*	*2*	*1*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*1*	*2*	*2*	*2*	*2*	*1*	*2*	*2*	*2*	43
5	*2*	*3*	*3*	*3*	*5*	*5*	*2*	*1*	*2*	*1*	*5*	*4*	*3*	*4*	*5*	*4*	*5*	*3*	*1*	*5*	*3*	*3*	*4*	76
6	*5*	*4*	*4*	*5*	*4*	*4*	*5*	*4*	*4*	*3*	*4*	*4*	*3*	*4*	*3*	*4*	*2*	*4*	*2*	*4*	*4*	*4*	*2*	86
7	*2*	*1*	*3*	*1*	*5*	*1*	*5*	*2*	*5*	*1*	*5*	*2*	*4*	*4*	*3*	*4*	*5*	*4*	*3*	*5*	*3*	*4*	*4*	76
8	*5*	*4*	*4*	*4*	*4*	*2*	*4*	*3*	*2*	*4*	*5*	*4*	*3*	*3*	*2*	*3*	*1*	*3*	*1*	*1*	*3*	*1*	*3*	69
9	*1*	*5*	*3*	*3*	*5*	*3*	*5*	*4*	*1*	*4*	*3*	*4*	*5*	*3*	*3*	*3*	*4*	*4*	*3*	*3*	*4*	*4*	*5*	82
10	*5*	*3*	*3*	*3*	*3*	*4*	*3*	*5*	*3*	*4*	*3*	*3*	*4*	*4*	*3*	*4*	*4*	*4*	*3*	*4*	*5*	*3*	*4*	84
11	*2*	*4*	*4*	*1*	*4*	*1*	*4*	*1*	*1*	*1*	*3*	*1*	*3*	*1*	*2*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	41
12	*5*	*3*	*5*	*3*	*5*	*5*	*3*	*5*	*3*	*4*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*4*	*3*	*2*	*4*	*4*	*2*	81
13	*2*	*2*	*2*	*2*	*2*	*1*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	45
14	*5*	*2*	*4*	*2*	*4*	*1*	*4*	*4*	*4*	*5*	*3*	*5*	*5*	*3*	*5*	*5*	*3*	*5*	*5*	*4*	*4*	*4*	*4*	90
15	*4*	*5*	*5*	*3*	*5*	*3*	*5*	*4*	*5*	*5*	*5*	*3*	*5*	*3*	*3*	*5*	*5*	*5*	*5*	*5*	*5*	*5*	*5*	103
16	*5*	*2*	*5*	*5*	*3*	*5*	*3*	*5*	*5*	*4*	*5*	*4*	*5*	*4*	*5*	*4*	*5*	*4*	*4*	*5*	*4*	*5*	*5*	101
17	*3*	*5*	*5*	*4*	*5*	*4*	*5*	*4*	*5*	*4*	*5*	*4*	*5*	*4*	*5*	*5*	*5*	*5*	*5*	*5*	*5*	*5*	*5*	107
18	*1*	*2*	*1*	*2*	*2*	*2*	*1*	*2*	*2*	*2*	*2*	*1*	*2*	*2*	*1*	*2*	*1*	*2*	*1*	*2*	*1*	*2*	*2*	38
19	*2*	*3*	*1*	*3*	*1*	*2*	*1*	*1*	*3*	*1*	*5*	*5*	*4*	*5*	*5*	*4*	*1*	*4*	*1*	*4*	*1*	*4*	*3*	64
20	*4*	*3*	*3*	*3*	*4*	*3*	*2*	*2*	*2*	*1*	*3*	*3*	*1*	*5*	*1*	*1*	*1*	*1*	*1*	*5*	*5*	*1*	*2*	57
21	*2*	*5*	*5*	*4*	*5*	*4*	*5*	*3*	*5*	*5*	*5*	*3*	*2*	*4*	*2*	*4*	*5*	*5*	*4*	*4*	*5*	*4*	*3*	93
TOTAL	70	71	76	63	77	64	74	66	65	67	81	68	72	74	65	73	67	74	61	76	74	69	69	
EDAD	27	28	41	21	40	22	39	22	22	21	25	39	31	30	22	25	45	32	36	54	29	49	52	
OCUPACIÓN	Estudiante	Ing. Sistemas	docente	estudiante	Ing. Sistemas	diseñador	contador	estudiante	Ing. Sistemas	estudiante	obrero	obrero	empleado	empleado	empleado	profesionista	profesionista	empleado	propietario	Lic. info.	estudiante	profesor	Obrero	