UNIVERSIDAD DEL AZUAY

FACULTAD DE ADMINISTRACIÓN

ESCUELA DE "INGENIERÍA DE SISTEMAS"

ANÁLISIS DEL FUNCIONAMIENTO, SEGURIDAD Y COSTOS DEL "CARRITO DE COMPRAS"

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERA DE SISTEMAS

AUTORES:

MARÍA BELÉN GALINDO GONZÁLEZ

GABRIELA ELIZABETH PARRA ROBLES

DIRECTOR:

ING. ESTEBAN CRESPO

CUENCA, ECUADOR

2014

Dedicatoria

A mis padres Pepe y Narcisa, por el apoyo incondicional que me han brindado pese a las circunstancias de la vida siempre me supieron respaldar y cumplieron con mi capricho de estudiar en la “UDA”, la carrera de “Ingeniería en Sistemas”, sin reprochar mi decisión estuvieron luchando junto a mí, caminaron de la mano conmigo hasta culminar esta meta anhelada; y hoy puedo decirles que la única manera con la que puedo pagarles todo esto es diciéndoles: “Mamá, Papá soy Ingeniera”; a mis hermanos Juanjo y Danny, quienes colaboraron con las idas a dejar e idas a ver sin mirar la hora; a toda mi familia que siempre estuvo pendiente y confió en mí; a mi Gordo Gustavo por la paciencia, el apoyo y sobre todo por jamás dejarme rendir; a todos quienes son considerados mis amigos, pues con su ayuda de alguna u otra manera colaboraron para que cumpla uno más de los objetivos de mi vida.

María Belén

Dedicatoria

La más grande de mis metas la dedico a mis papis Cathy y Pachi, pues son ellos quienes guían mis pasos, con quienes celebro mis triunfos y quienes me tendieron la mano cada vez que me caía, demostrándome que con amor, constancia y perseverancia puedo llegar muy lejos.

A mis hermanas Natu y Taby, mis nenas, las que con tanto cariño y ternura están siempre apoyándome y con la alegría que les caracteriza, ayudándome a ser una mejor persona.

A mi abuelita Bertita, porque jamás le faltó una palabra de aliento para impulsarme a conseguir ésta meta.

A toda mi familia y amigos, sin ustedes, mi vida no sería la misma.

Gabriela Elizabeth

Agradecimiento

Queremos agradecer a Dios, por darnos todos los dones que poseemos, por encaminarnos hacia el triunfo y a pesar de las adversidades y obstáculos presentados en el camino, siempre sentimos su presencia en nuestros corazones.

A nuestros padres, porque gracias a su apoyo, consejos y amor incondicional, logramos culminar con éxito otra de las etapas de nuestras vidas.

Inge Esteban, gracias, mil gracias porque más que profe, se convirtió en un gran amigo, nos enseñó a enfrentarnos a nuevos retos, a unir la teoría y ponerla en práctica, a tomar decisiones; porque usted creyó en nosotras y accedió a ser el tutor de sus alumnas más “molestosas”, pero queridas. Muchas gracias Inge, de todo corazón.

Queremos agradecer a las personas que nos hicieron pasar tantas malas noches, los que nos llenaron de proyectos interminables, y con quienes disfrutamos los triunfos; a nuestros profes, porque cada uno, contribuyó para que hoy seamos unas profesionales exitosas.

Muchas gracias

Resumen

La evolución de la tecnología informática ha obligado a las PYMES a adoptar al comercio electrónico como una nueva ventaja competitiva, mediante la implementación de un carrito de compras y un botón de pagos; para ello la organización debe analizar los costos, porcentajes y políticas que sustentan cada uno de los mecanismos de pagos más reconocidos a nivel mundial: Paypal, Visa y MasterCard, así como un estudio de la seguridad mediante el modelo de calidad ISO 25010; ya que de no contar con éstas normas, el tarjetahabiente y el comerciante están propensos a sufrir fraudes electrónicos.

ABSTRACT

The evolution of computing technology has mandated that Small and Medium Sized Enterprises (SMEs) adapt to e-commerce as a new competitive advantage through the implementation of a shopping cart and a payment button. To do this, the organization must analyze costs, percentages and policies that support each of the payment mechanisms recognized worldwide: Paypal, Visa and Mastercard, as well as a security study using the quality model ISO 25010. Failure to achieve these norms can lead to the propensity for cardholders and merchants to become victims of electronic fraud.

UNIVERSIDAD DEL AZUAY
DPTO. IDIOMAS

Translated by

Ing. Melita Vega

August 7, 2014

Índice de contenidos

Índice de Tablas

Índice de figuras

CAPITULO 1. E-commerce en la actualidad

1.1 Introducción

En la actualidad, el motor que ha generado un cambio radicalmente es el desarrollo y crecimiento de las nuevas tecnologías de la información, las cuales han marcado grandes cambios en los procesos de compra y venta de bienes y/o servicios permitiendo la creación del método de pago electrónico, brindando mayor rapidez en la prestación del servicio.

El negocio electrónico brinda nuevas formas de comercializar, haciendo más eficiente y eficaces sus operaciones internas, ventas y comercialización, estrategias de mercadotecnia y administración; por ésta razón, varias son las empresas que se plantearon un modelo electrónico como ventaja competitiva, logrando así un giro empresarial.

Las pequeñas y medianas empresas son las que deberán adaptarse al uso de las nuevas tecnologías, aplicaciones y procedimientos, pues si bien es cierto no serán únicamente las grandes empresas las que triunfen, sino todas aquellas que logren adecuarse a las nuevas tecnologías, pues su éxito dependerá del enfoque y de cómo éstas contribuyan a los procesos de negocios.

El impacto que tiene el e-commerce es trascendental en ésta época, genera éxito empresarial y oportunidades de mejora en la prestación de un servicio, es por esto que las empresas tradicionales deben integrarse al conjunto de mercados digitales, caso contrario se quedarán fuera de competencia.

Está nueva forma de negociar, así como tiene las ventajas de rapidez, comodidad, minimización de costos, trae consigo una serie de problemas, riesgos y fraudes informáticos que pueden afectar notablemente al desempeño de la actividad comercial, destacando el robo de información confidencial del tarjetahabiente.

Por la razón antes mencionada, las entidades financieras han visto la necesidad de implementar diversos métodos de seguridad para salvaguardar la información de los usuarios, entre los cuales sobresalen los criptogramas, que cifran datos personales y contraseñas a través de diferentes algoritmos.

Si bien, en la actualidad la seguridad es cada día más robusta y los riesgos poco a poco pueden ser controlados, se debe tener igual o más cuidado que antes, ya que siempre es un peligro transmitir información a través de medios electrónicos, sin embargo, los usuarios hoy en día realizan sus transacciones en línea con mayor confianza, pues las compañías bancarias han implementado métodos de protección de información y autenticidad, a través de un código alfanumérico denominado PIN.

El PIN, que es requerido al momento de presionar el botón de pago en el portal web, permite identificar inequívocamente si dicha persona es la dueña de la tarjeta a utilizar; siendo éste proceso en Visa denominado Verified by Visa, SecureCode en MasterCard y en eBay como Paypal.

Conociendo la factibilidad que tendrá un negocio que cuenta con un carrito de compras, se analizará a fondo las ventajas y desventajas de cada uno de los organismos financieros, así como los costos y políticas de seguridad implementados por los mismos, con el único objetivo de comparar y tener una referencia real según análisis Costo-Beneficio e ISO 27001, y poder elegir con cuál de dichas

organizaciones se querrá aplicar los métodos y medidas necesarias para llevar a cabo el carrito de compras en un negocio tradicional.

1.2 Desarrollo de la estructura del comercio electrónico.

1.2.1 Definición del e-commerce.

El e-commerce o "comercio electrónico", es una tecnología que requiere la utilización de internet como canal para la realización de varias actividades involucradas en la gestión de los negocios, es decir para la compra y venta de productos y/o servicios con proveedores o consumidores, manejo de la cadena de producción, el e-marketing, elaboración de trámites bancarios como pagar, cobrar, transferencias electrónicas de fondos; involucrando así todas aquellas operaciones que requiere el comercio a través de diversos dispositivos electrónicos.

El e-commerce se tiene entre negocios, consumidores y el gobierno, creando así los diferentes tipos de comercios electrónicos, entre los cuales se tiene:

- Business to Business (B2B): Comercio realizado entre empresas, es decir de empresa a empresa.
- Business-to-consumer (B2C): Es el comercio que se realiza entre la empresa productora, vendedora o prestadora de servicios y el consumidor final.
- Consumer to Consumer (C2C): Se refiere a la forma de realizar comercio electrónico entre usuarios de internet sin involucrar a productores y sin intermediarios.
- Government to Consumer (G2C): Es el comercio que se realiza entre el gobierno y los consumidores; en la actualidad este tipo de negociación es uno de los más utilizados, por ejemplo en el pago de impuestos, multas y tarifas públicas.

- Government to Business (G2B): Este tipo de comercio se lo usa para los negocios entre gobierno y empresas, por ejemplo: en el concurso de precios para alguna obra pública.

La mayoría de PYMES ecuatorianas utilizan el e-commerce como ventaja competitiva, sabiendo que es una inversión a corto plazo, ya que para contar con este servicio se requiere un responsable del comportamiento de la empresa en Internet, un equipo de especialistas en e-commerce dedicados al marketing, diseño y programación de distintas funciones, entre las cuales sobresalen el colocar el catálogo completo de los productos o servicios que presta la empresa de forma llamativa y original, mostrando un stock completo de la mercadería con la que cuentan y sus respectivas actualizaciones; facilitando el contacto con los usuarios y atendiendo todos sus requerimientos.

Todas estas acciones y decisiones aumentarán la satisfacción del consumidor, logrando así mantenerlos y conquistando nuevos usuarios, de ésta manera la empresa recuperará todo lo invertido y tendrá grandes remuneraciones.

Existen cuatro aspectos importantes para llevar a cabo satisfactoriamente la acción del e-commerce, los mismos se los debe considerar al momento de personalizar las tiendas on-line, ya que serán los que permitan tener mayores ventajas competitivas, éstos son:

- Privacidad: Es el aspecto más importante, pues los usuarios desean que su información sea manejada de forma cautelosa, por lo que se debe ejecutar procesos de privacidad en las compras, todo de acuerdo a las Leyes de Comercio Electrónico vigentes.
- Físico: Esta característica debe tener toda página de un portal web, pues tiene la capacidad de llevar los online a lo offline, a través de una correcta

integración de la información que generan los medios online a las diversas tiendas.

- Predictivo: El comercio electrónico debe tener procesos proactivos, es decir adaptarse a los intereses de compra de los clientes, logrando así la satisfacción del consumidor.
- Proactivo: Además de brindar la opción de comprar bienes y/o servicios, el portal web incentivará al cliente brindándole información y servicios digitales, en un formato personalizado.

El denominado "Carrito de Compras" dentro del comercio on-line es una herramienta tecnológica que ayuda a los usuarios a la adquisición de productos y/o servicios, de una manera fácil y sencilla, luego de que los mismos hayan ingresado sus datos, confirmado los productos escogidos y enviado el pedido; seguidamente del proceso de pago, donde el cliente puede elegir la forma de realizar la transacción que más le convenga, a fin de que se proceda a la verificación y validación de sus datos, para culminar con éxito su compra.

Para que este proceso ocurra eficientemente, el punto más importante es la calidad del sitio web, empezando con un buen diseño que incluya facilidad de navegación y que sea intuitivo, sin abundante publicidad y con variedad de productos y/o servicios;, la confianza, la seguridad y las diferentes formas de pago son los pilares fundamentales para que exista un buen comercio electrónico.

1.3 Estrategias del mercado.

Se puede decir que una buena estrategia es aquella que permite asegurar el ingreso del producto o servicio al mercado, aumentando las ventas a través de la red;

siendo necesaria la elaboración de un plan a corto o mediano plazo, donde se describa el proceso para llegar al objetivo propuesto. *Para ello es conveniente estudiar el mercado, y preguntarse: ¿Con qué productos se entrará a la Web? ¿A quiénes se dirigirá la empresa? ¿A dónde se quiere llegar? ¿Cómo se lo hará?* (Plan de Marketing. 2003. Estrategias de Mercado. 6 Octubre 2013. http://www.guia.ceei.es/interior.asp?MP=8&MS=7)

Una vez que se responda a estas preguntas, es necesario plantear estrategias claras, que contribuirán con la creación e implementación de la empresa que se manejará vía online, dando lugar al comercio electrónico, de esta manera la empresa se podrá dar a conocer y poco a poco penetrar en el mercado, ya sea para beneficio o simplemente sirviendo de experiencia para los creadores de la misma.

Es muy probable que empresas fracasen al inicio o con el pasar de los días, puesto que no manejaron bien el proceso para llegar al objetivo planteado en un principio. A continuación se detallan estrategias que ayudarán a obtener un buen resultado a las empresas que ingresan en el mundo cibernético.

Uno de los aspectos principales para que el comercio electrónico salga adelante es la página web, ya que dará a conocer a los clientes y/o usuarios los productos y servicios que ofrece la empresa. Ésta debe cargarse de manera rápida para que las personas puedan revisarla, así como también contener material interesante, debe ser intuitiva, atractivamente gráfica, de fácil manejo y de constante actualización respecto a sus contenidos, teniendo la información suficiente para el interés de los compradores.

Es primordial que la página o portal web ofrezca la seguridad que el cliente necesita para realizar la compra y de esta manera se pueda confiar en el pago sin problema alguno. Además se deben elegir perfectamente las palabras claves

(metadatos) para que la página esté disponible inmediatamente al momento de la búsqueda en la web, relacionando los productos de forma correcta para que le usuario encuentre lo requerido y no tenga que abandonar el portal por la carencia y fallas en la búsqueda.

Otro aspecto que es beneficioso para la empresa online es la publicidad, siendo una herramienta clave para el conocimiento de la misma, teniendo en cuenta que conforme avanza la tecnología más posibilidades se tiene para que las personas conozcan el ingreso al mercado de una nueva empresa, cabe recalcar que hoy en día uno de los métodos más utilizados para la publicidad es manejar la información mediante las redes sociales, permitiendo que la empresa sea reconocida en el país de origen y por qué no a nivel mundial; es importante hacer que el cliente se fidelice con la empresa, poniéndole boletines de información que llamen su atención, mandando correos refiriéndose a promociones, mostrándole la facilidad de pago, y haciéndole sentir parte de la organización comercial. La empresa se abre camino y se da a conocer dando auspicios, mostrándose en la prensa, radio, televisión, banners informativos, siendo estos llamativos para que capte la atención de las personas.

Es importante estar al tanto de la competencia ya que probablemente se tenga que bajar precios o aumentar ofertas para disputar las ventas, esto quiere decir, la empresa que menor costo ponga en los productos o servicios disponibles será la que obtenga la compra.

Existen clientes que por varios motivos realizan la compra solo mirando el producto vía online, pero hay otros que utilizan la página web de la empresa como catálogo pero que necesariamente necesitar observar y manipular el producto por ellos mismos, es por eso que una estrategia para no perder al comprador es tener un lugar físico a donde éste pueda ir y sentirse satisfecho con el producto elegido, y que

al instante realice su compra; en caso de no tener la infraestructura físicamente es necesario brindar la información detallada con la más mínima característica para así convencer al cliente del producto que más le llame la atención.

1.4 Problemas Presentados.

El e-commerce en la actualidad es una de las más grandes ventajas competitivas que puede tener una PYMES; éstas saben que dicho comercio es una realidad accesible y eficaz para crear canales de venta con un futuro exitoso y posibilidades de internacionalización. La implementación del mismo es fácil, pues puede estar basada en unas de las tantas plataformas tecnológicas de comercio electrónico que se encuentran de forma gratuita en Internet; sin embargo, lo importante es hacer que las necesidades del cliente en los distintos negocios encajen con dichas plataformas y a partir de ello sacar el máximo rendimiento en las ventas.

A pesar de las grandes ventajas que trae consigo un comercio electrónico, éste tiene varios problemas que surgieron con la creación del mismo, pero que algunos de ellos con el paso de los años han podido solucionarse parcial e incluso totalmente, entre los inconvenientes más destacados y con mayor disgusto de los usuarios, se puede mencionar:

- La confiabilidad en el servicio post venta, pues la falta de ésta en los usuarios disminuirá notablemente la concurrencia de compradores en el portal web, se debe tener principal atención y seguir el proceso del cliente tras la compra de un producto, ya sea por si se trata de una devolución, un cambio, por si surgiese algún inconveniente con los productos o servicios contratados, o simplemente para aceptar los sentimientos de satisfacción del mismo

- El tiempo de respuesta de la página web, pues al aumentar la popularidad de los portales, aparecen varios aspectos negativos como la incrementación del tráfico, por lo tanto a mayor demanda de usuarios, mayor tiempo de espera en la carga de dichas páginas, lo que provoca la insatisfacción en el usuario.

  Se debería controlar este inconveniente gestionando los tiempos de respuesta, ya que no se desea que los clientes potenciales abandonen la tienda virtual, y la misma baje su reputación; causando así la reducción de ventas y como consecuencia mayor la disminución de ingresos.

  Según estudios de Borland Software Corporation (compañía Micro Focus que identifica los requisitos, pruebas y gestión de cambios), el promedio de tiempo que un comprador on-line da al portal para que se cargue es de 2 segundos, pasado dicho tiempo está dispuesto a esperar otros 3 segundos más; y después de esa espera un 40% de los usuarios abandonan la página; por otro lado los clientes que acceden a las tiendas virtuales a través de un dispositivo móvil, esperan como máximo 5 segundos para que la página empiece a cargarse, pasado este tiempo, el 74 % de los mismos deciden abandonar el sitio web.
- La interfaz Web consiste en un conjunto de elementos gráficos que permiten al usuario acceder a los contenidos, navegar e interactuar a través de la computadora, o dispositivo móvil; éstas deben ser lo más sencillas e intuitivas, sin descuidar un diseño estético que llame la atención del cliente, recordando que la simplicidad y comodidad son los dos principios fundamentales para el desarrollo de una interfaz efectiva, logrando así que el usuario continúe navegando en el portal y vuelva cada vez que necesite otro producto o servicio.

Se debe evitar la publicidad e imágenes molestosas, archivos de sonido y programas que puedan bloquear al navegador del visitante; pues provocan retraso en la carga del portal web y hacen las páginas más pesadas.

El portal debe contar con una estructura organizada de la información, de manera que el usuario pueda acceder a ésta con facilidad; además se requiere de una interfaz intuitiva que contenga buscadores, menús e información relevante para el cliente.

Cabe recalcar que los componentes más importantes de la interfaz son los contenidos, la estética y la funcionalidad, y lo importante es lograr un equilibrio entre éstos, así se obtendrá que los usuarios incrementen y que no acudan al portal web sólo para comprar, sino para interesarse de los productos que presente el mismo.

- La protección de datos, ya que Internet por el mismo hecho de ser un medio libre y gratuito, no tiene control y facilita la trasmisión e intercambio de datos de manera sencilla. Por tal motivo el portal web debe velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, de manera que la misma proteja la identidad de cada usuario del comercio electrónico.

  Al hablar de protección de datos se hace referencia a la seguridad de derechos de información, acceso, rectificación, oposición; teniendo en cuenta que en caso de ilegalidad, se dará el cese en el tratamiento y la cancelación de los datos, así como la obligación de los portales de tutelar los derechos y garantías de los usuarios.

- Manejo del e-mail, pues se deberán enviar noticias a los potenciales clientes; información que sea requerida y que tenga sentido para el usuario, pues el envío de

comunicaciones comerciales no solicitadas (spam) lo molestan y exigen a que el portal sea marcado como no deseado.

El correo que se envía debe tener una cabecera donde el asunto del mensaje tiene que ser claro y conciso; y, el cuerpo del mismo estar muy bien detallado, sin errores de deletreo, problemas gramaticales, y muy fácil de leer.

- Usar proveedores de hospedaje gratuitos, ya que éste muchas veces tomará el control absoluto del sitio web, poniendo restricciones sobre sus servicios, pues puede limitar el tráfico del portal, el almacenamiento, y la preferencia de distintos formatos de archivos. La mayoría de estos host no ofrecen soporte técnico de calidad y no se responsabilizan por el funcionamiento del sitio web; en caso de que el servidor caiga y se averíe algún disco duro, recurren al punto de restauración, recuperando información almacenada en los distintos intervalos de tiempo.

1.5 Ventajas y desventajas.

Siendo el e-commerce una transacción comercial implementada para la venta de productos y servicios mediante Internet, considerada como el nuevo marco de negocios que ayuda a satisfacer las necesidades tanto de las empresas como de los usuarios, reemplazando a las operaciones manuales basadas en papel por la alternativa electrónica; ofrece importantes beneficios y al mismo tiempo representa riesgos.

1.5.1.1 Ventajas que tiene el Usuario a través del e-commerce:

- Encontrar con facilidad y comodidad un producto o servicio a menor precio, durante las 24 horas, los 7 días a la semana y sin necesidad de trasladarse hacia la empresa.

- Comparar precios y calidad de productos de manera rápida, ya que puede navegar en páginas de varios vendedores y comprar en la de mejor oferta.
- Disponer de confidencialidad y fácil acceso a la adquisición de lo solicitado.
- Acceso a mayor información de lo requerido, es decir se dará a conocer de una manera más profunda el producto o servicio.
- Tener la facilidad de consultar y aclarar vía online de una manera efectiva todas las inquietudes, obteniendo soporte técnico inmediato o en un futuro.
- El usuario se mantendrá informado sobre la empresa y sus productos.
- Contar con mecanismos de comodidad y flexibilidad para cancelar sus compras, pues existen diferentes tipos de pagos.

1.5.1.2 Ventajas que tiene la empresa a través del e-commerce:

- Los proveedores pueden ingresar a un mercado iterativo en donde los costos tienden a cero.
- Socializan unas empresas con otras, realizando negocios y obteniendo beneficios a corto y largo plazo, hechos que con métodos tradicionales quizá y no hubiese sido posible.
- La empresa ahorra pues no posee obligaciones con empleados.
- Existiría seguridad física, puesto que ya no se darían las perdidas por mercadería robada.
- No existirán ventas perdidas en los días feriados o de descanso.
- Habrá mayor ganancia por la venta unitaria de los productos o servicios.
- Se dará a conocer la empresa nacional o internacionalmente y se incrementará en un futuro innumerablemente las ganancias mediante este medio.
- Podrá brindar un servicio innovador y de un mayor agrado a los clientes.

- La empresa entrará a competir a nivel mundial en donde las condiciones son iguales ya que el cliente no sabe si la empresa es grande o no.

Luego de haber concluido con lo beneficioso que puede resultar el comercio electrónico para la sociedad se citarán obstáculos o desventajas que aunque son pocos van de la mano con el e-commerce:

1.5.1.3 Desventajas del Usuario respecto al e-commerce:

- En caso de inconvenientes e inconformidades con el producto, el comprador no tendrá la posibilidad de reclamar directamente al vendedor.
- La visualización del producto no existe, siendo importante para la compra de mercadería.
- Existe temor en los usuarios, pues no hay quien les garantice o guíe en las compras y pagos por internet.
- En ciertos portales, una vez adquirido el producto, se pierde el derecho a reclamar en caso de ser necesario.

1.5.1.4 Desventajas de la Empresa respecto al e-commerce:

- No hay la comunicación entre los vendedores y los clientes.
- Se tiende a atraer a los hackers y crackers que hacen un mal ya sea en el momento de realizar una venta o una compra, por lo tanto las empresas pierden sus clientes.
- La empresa puede ser estafada ya que no se sabe si la persona que se registra y realiza una compra realmente es quien dice ser.
- En caso de que se presente una página que contenga un idioma diferente al que maneja el usuario es muy probable que éste evite ingresar a realizar compras en la misma.

- Por la falta de educación solo una parte de la población tiene acceso a Internet y por lo tanto desconoce el manejo del comercio electrónico, es por eso que afecta de alguna u otra manera a que las empresas se hagan conocer completamente alrededor del mundo.
- En caso de que la empresa no esté constituida legalmente pierde el conocimiento total de las personas que utilizan el comercio electrónico ya sea dentro o fuera del país.

CAPITULO 2. Carrito de Compras

2.1 Análisis del funcionamiento del Carrito de Compras

2.1.1 Definición del funcionamiento.

El carrito de compras es una aplicación de gran ayuda y facilidad para que el usuario pueda adquirir sus bienes o servicios mediante la comodidad de su hogar, a través de un dispositivo electrónico y una conexión a Internet para poder ingresar al portal web, en donde se podrá elegir y agregar al carrito de compras uno o varios artículos.

La página del carrito de compras lista todos los productos seleccionados por el usuario con un detalle de los mismos y su subtotal, logrando así la seguridad del cliente al momento de escoger sus compras. Dicha página debe:

- Permitir al usuario vaciar todos los artículos del carrito de compras, en el momento en el que éste se arrepienta de realizar su compra, solo deberá pulsar el botón “vaciar carrito”, y en ese momento la lista desaparecerá.
- Actualizar la cantidad de cualquier producto de la lista, en caso de que se desee agregar o quitar el número de artículos seleccionados; cabe recalcar que en el momento que se cambia la cantidad, ésta se actualizará y el subtotal se deberá recalcular.
- Reconocer el abandono de la compra por parte de los usuarios después de haber agregado distintos productos al carrito de compras, de esta manera no se modificará el inventario.
- Contar con una opción que permita al usuario “continuar comprando”, es decir regresar a la página donde se encuentran los artículos, y dar libre acceso para que los clientes puedan escoger más artículos.

- Acceder a una página donde se procederá a realizar el pago pertinente; para el cual primero se debe recogerla información del cliente y se mostrará las condiciones de pago, además, resume la orden proporcionando el costo total. El usuario deberá enviar datos personales sobre un canal seguro en esta página.
- Confirmar a través de un mensaje al cliente que la orden fue exitosamente guardada. Se deberá proporcionar un número de referencia al usuario incluyendo el detalle de la lista de la orden (productos, cantidades, precios, totales, fecha de compra).

2.1.2 Importancia en los negocios electrónicos

El crecimiento del comercio electrónico se ha logrado por al aumento de las conversiones on-line, y esto se realizó gracias a la implementación de los carritos de compras. De aquí nace la importancia de los mismos, pues se han convertido en la aplicación más reconocida por empresas pequeñas y grandes, ya que ha llevado a un creciente número de solicitudes concurrentes en el mercado.

Una de las expectativas de toda tienda virtual es el de transformar el tráfico de su sitio web en ventas. Para ello primero debe atraer tráfico e invertir en publicidad, ya que da el potencial de posicionamiento y las ganancias en línea; si el comercio cuenta con suficiente tráfico y no logra convertirlo en ventas, esa demanda de visitantes y el gasto en publicidad fue inútil.

Para que los clientes no sean únicamente visitantes y se conviertan en consumidores activos, es importante llamar la atención con una aplicación que despierte su interés en el portal web, la misma que deberá ser un carrito de compras,

fácil de navegar y lo suficientemente flexible para atender todas las necesidades requeridas por los usuarios.

El funcionamiento de un carrito de compras sigue exactamente los mismos procesos que los canastos de compras físicos en cualquier supermercado, con la única diferencia de que no existen límites en el horario para realizar la compra virtual.

Los procesos de compra son simples, ya que el cliente únicamente debe visitar y recorrer la tienda llenando el carro, controlando el precio de cada producto y costo final en la caja; pero para ello la tienda on-line debe contar con un "carrito de compras" eficiente, llamativo, rápido y sencillo, el mismo que deberá estar ubicado en una posición estratégica para no pasar desapercibido y del cual hay que cuidar siempre el diseño, pues, de ésta manera se incitará a la compra.

Como es normal en la conducta de todo ser humano, cuando se encuentra ante diversas opciones tiende a comparar, es por tal motivo que el cliente juzgará cada una de las tiendas on-line; es por ello, que éste sin duda es el mayor de los obstáculos que deberán atravesar los negocios virtuales, para obtener mayor cantidad de clientes potenciales, precisamente por esto, el carrito de compras adquiere gran relevancia y es de vital importancia para cualquier e-commerce.

Se debe tener mucho cuidado con los siguientes errores habituales en el diseño del carrito de compras, pues podrían marcar la diferencia:

- **Poca calidad en el diseño del carrito de compras:** éste debe ser atractivo, fácil de usar, muy intuitivo, simple; para así la tarea de comprar se convierta en un placer para el cliente; cabe recalcar que para que sea atractivo no

necesariamente debe ser demasiado llamativo, pues se lo puede confundir con la publicidad molestosa que aparece en cualquier página web. Un diseño simple, original, visible lograrán brindar confiabilidad al cliente para proceder a realizar sus compras. Y se debe tener especial cuidado con que el ícono del carrito, parezca realmente un "carrito de compras", pues un ícono o dibujo mal realizado o de muy baja calidad, hablará pésimo del negocio on-line.

- **Procesos realizados en el carrito de compras duren tiempos muy largos:** Existe una regla denominada: "*La regla de los 3 clicks"*, la misma que tiene sus bases en el diseño web refiriéndose específicamente a la navegación de un portal; según Jeffrey Zeldman en su libro, *Obtén tu talento en la web* (2001) afirma que "*La regla te puede ayudar a crear sitios intuitivos y con estructuras lógicas jerárquicas*"; y, explica que el usuario debería poder acceder a cualquier información del mismo en solo 3 clics a partir de la página de inicio; pues se dice que una mayor cantidad de clics para acceder a lo buscado causaría malestar y pérdidas, pues al usuario no le gusta esperar, por lo que abandonaría la página rápidamente; además que un proceso de larga espera crea desconfianza en los clientes.
- **Carrito de Compras que no cuente con ayuda**: La mayoría de usuarios que realicen compras on-line por primera vez, y uno que otro consumidor, necesitaran algún tipo de ayuda, pues es muy probable que tengan problemas en el momento de realizar una compra en una tienda on-line; por lo cual sería de gran utilidad que el sitio web cuente con procesos que le solucionen los conflictos, así el cliente sentirá satisfacción y agradecimiento por e-commerce.

Tener un carrito de compras en el portal web asegura que éste se trata de un e-commerce sofisticado y fácil de usar; se convertirá en una gran ventaja competitiva y afirmará las ganancias al transformar el tráfico de clientes visitantes en clientes consumidores.

2.1.3 Modelado de la Estructura del Carrito de Compras en UML

2.1.3.1 Diagramas de Comportamiento

Los diagramas de comportamiento se emplean para especificar, construir, visualizar y documentar la secuencia de estados por los que atraviesa un objeto de un sistema de software a lo largo de su trayectoria en respuesta a diferentes eventos.

Estos diagramas, pueden tener secuencias de estados simples y compuestos, llamados también aspectos dinámicos de un sistema de software, los mismos que son consecuencia de transiciones con eventos y diversas acciones.

Para entender el comportamiento y la transición de los diferentes estados de un carrito de compras, se realizaron los siguientes diagramas:

2.1.3.1.1 Diagrama de Actividad

2.1.3.1.1.1 Ingreso Compra

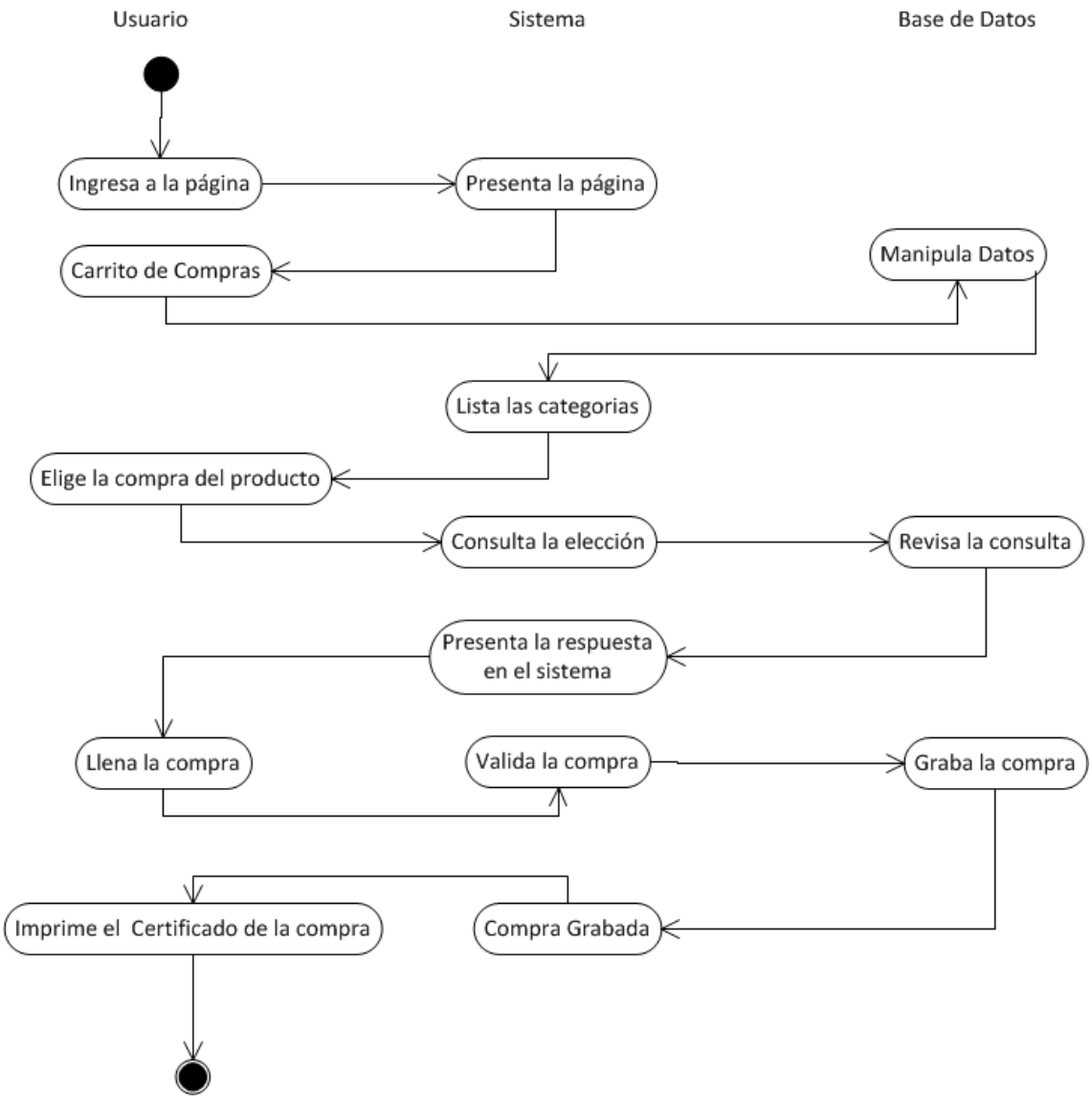


Figura 1 Diagrama de Actividad. Ingreso de Compra, (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.1.2 Modificar Compra

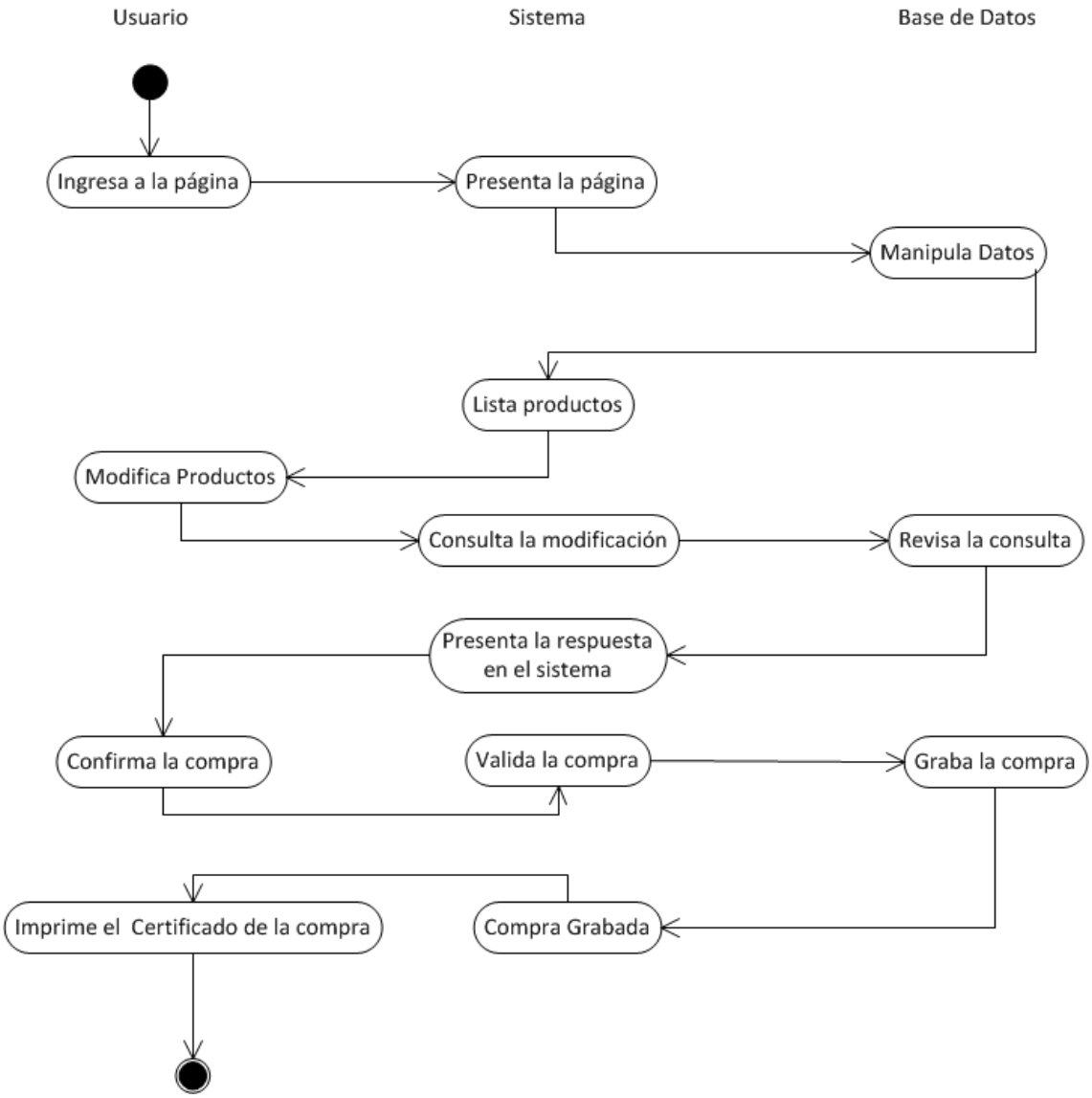


Figura 2. Diagrama de Actividad. Modificar Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.1.3 Vaciar Compra

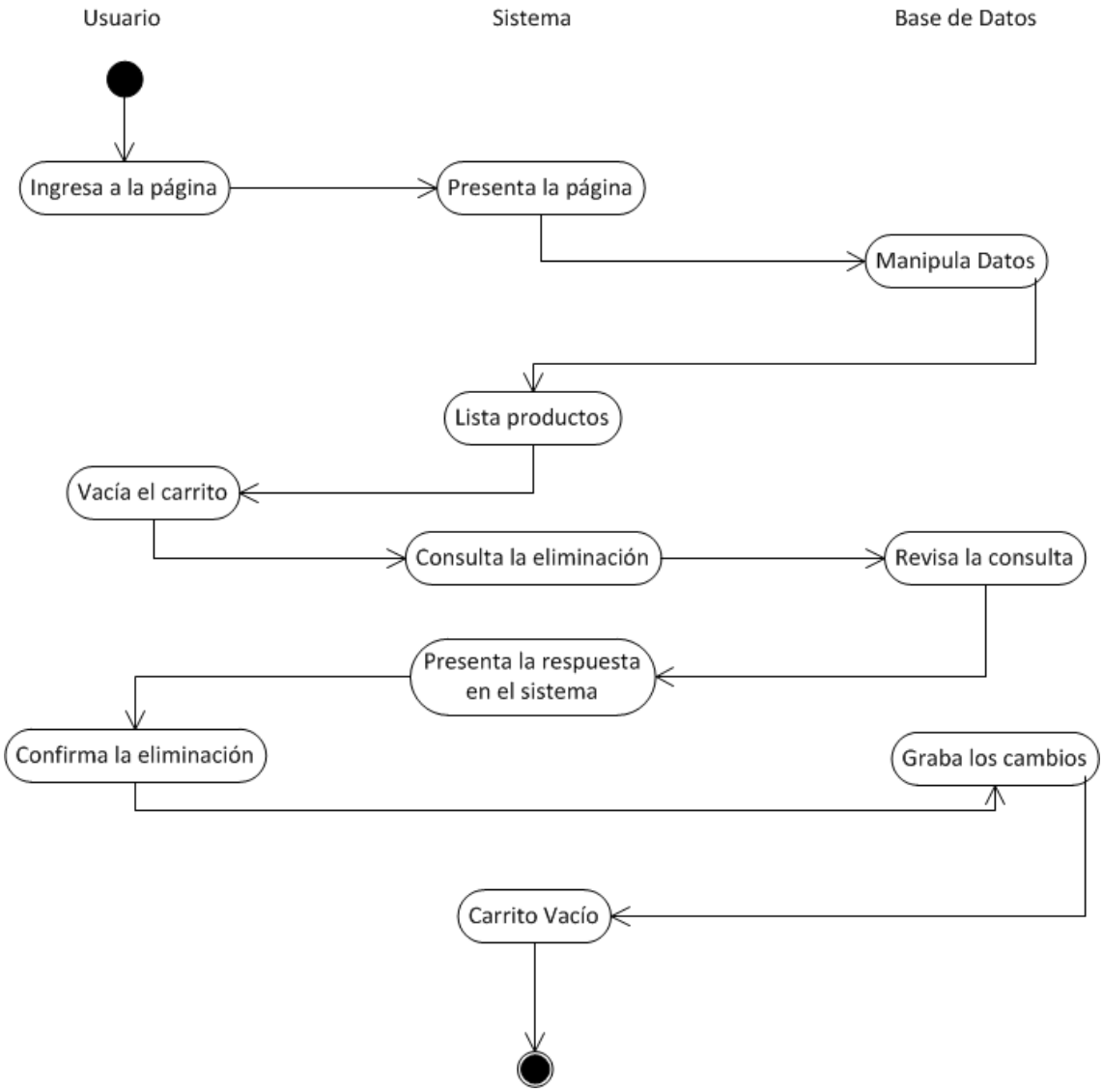


Figura 3. Diagrama de Actividad. Vaciar Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.2 Diagrama de Estado

2.1.3.1.2.1 Ingreso Compra

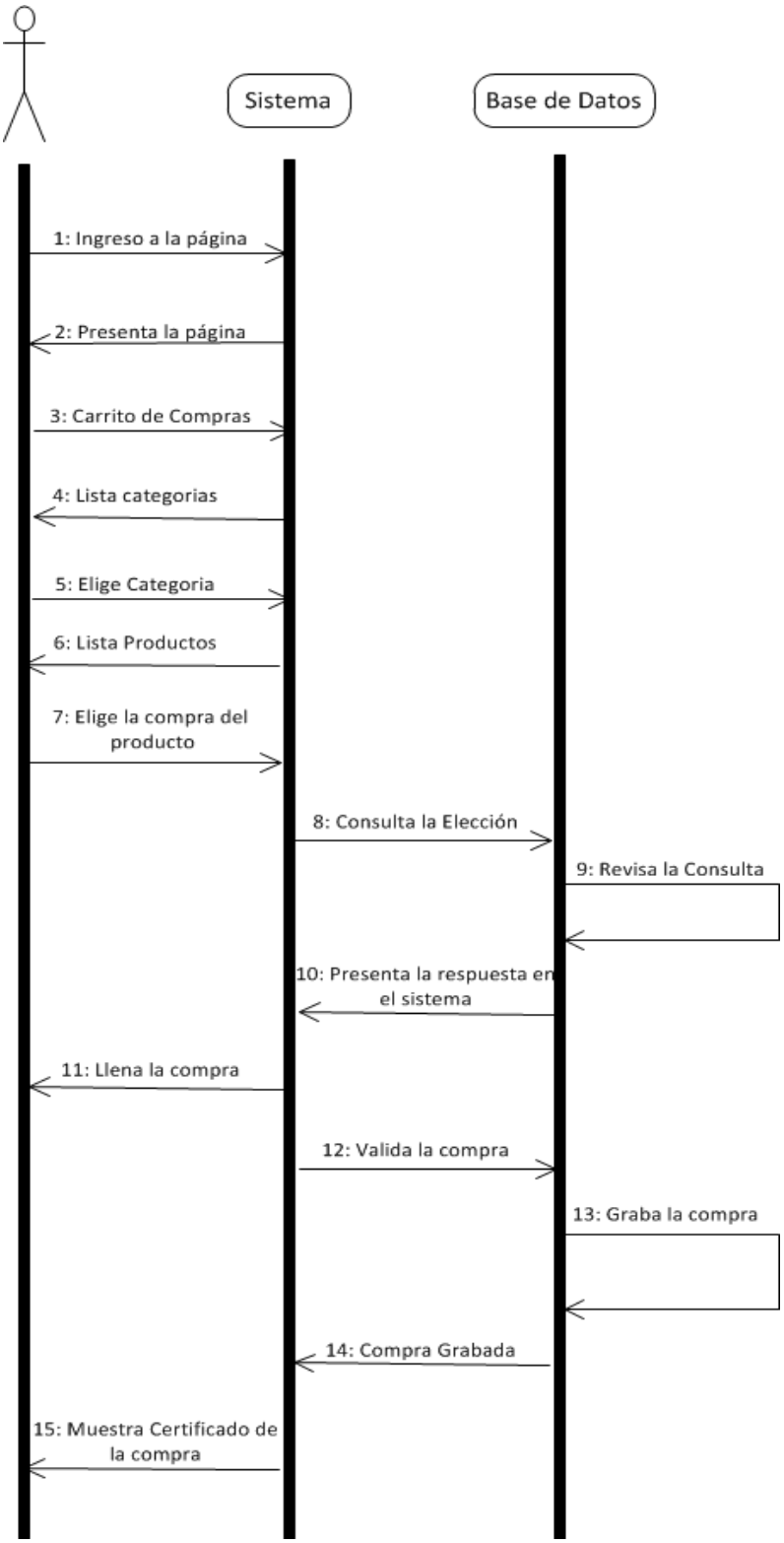


Figura 4. Diagrama de Estado. Ingreso Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.2.2 Modificar Compra

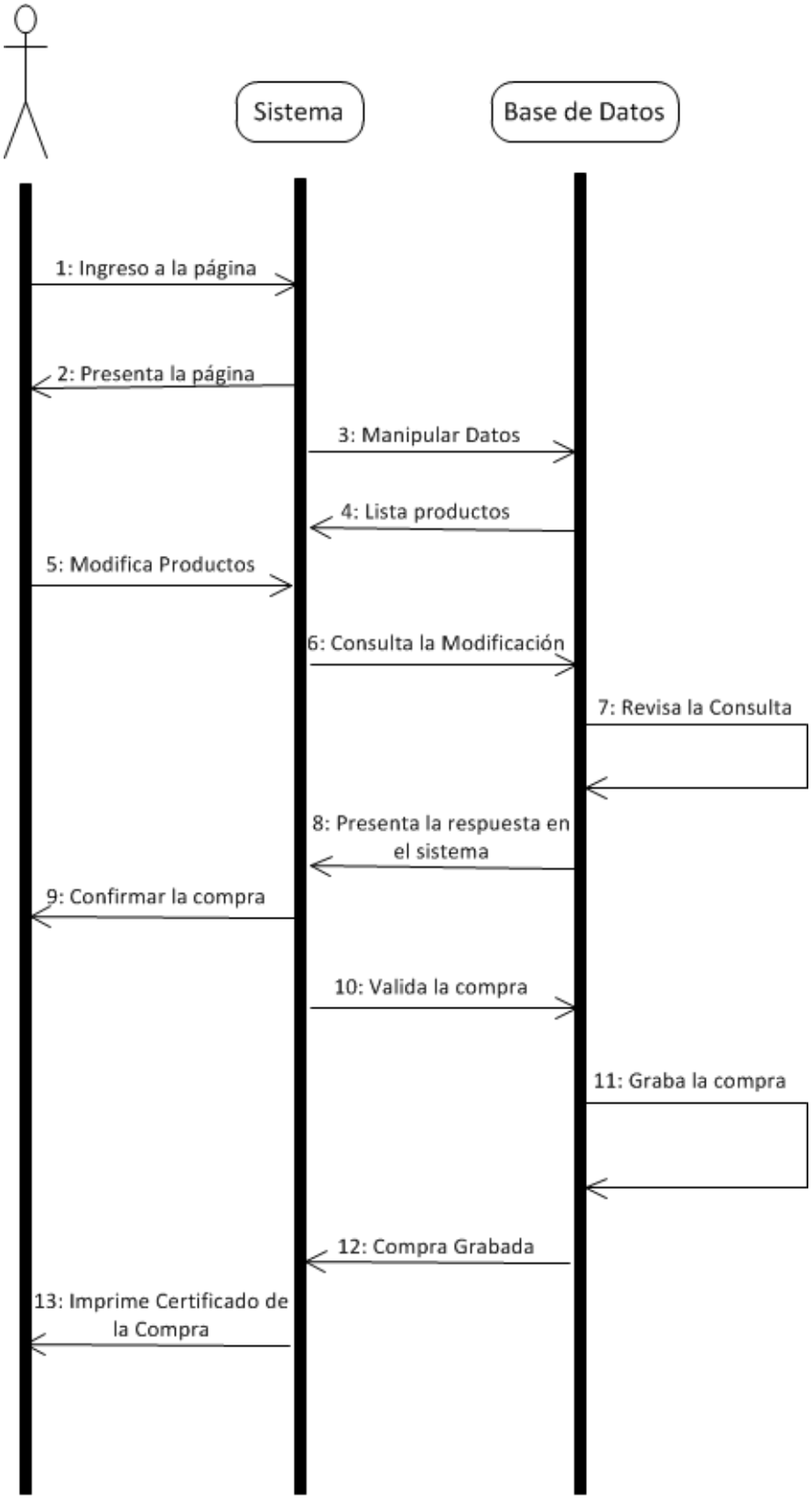


Figura 5. Diagrama de Estado. Modificar Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.2.3 Vaciar Compra

Figura 6. Diagrama de Estado. Vaciar Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.3 Diagrama de Casos de Uso

Figura 7. Diagrama de Casos de Uso (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.4 Diagrama de Interacción

Este diagrama puede ser obtenido desde el modelado de Clases o de Casos de Uso, y representa la forma en como un Cliente (actor, en el diagrama de Casos de Uso) u Objetos (Clases, en el diagrama de Clases) se comunican entre sí en petición a un evento, es decir describe la manera en que colaboran los objetos para cierto comportamiento, esto requiere un recorrido de la secuencia de llamadas, consiguiendo así las responsabilidades.

Los componentes de un diagrama de interacción son:

- Objeto (Diagrama de Clases) o Actor (Diagrama de Casos de Uso).

- Mensaje de un objeto a otro.
- Mensaje de un objeto a sí mismo.

Las diferentes interacciones entre objetos, que son respuestas a eventos, del funcionamiento del Carrito de Compras se modelaron en el siguiente diagrama:

2.1.3.1.4.1 Diagrama de Secuencia

2.1.3.1.4.1.1 Ingreso Compra

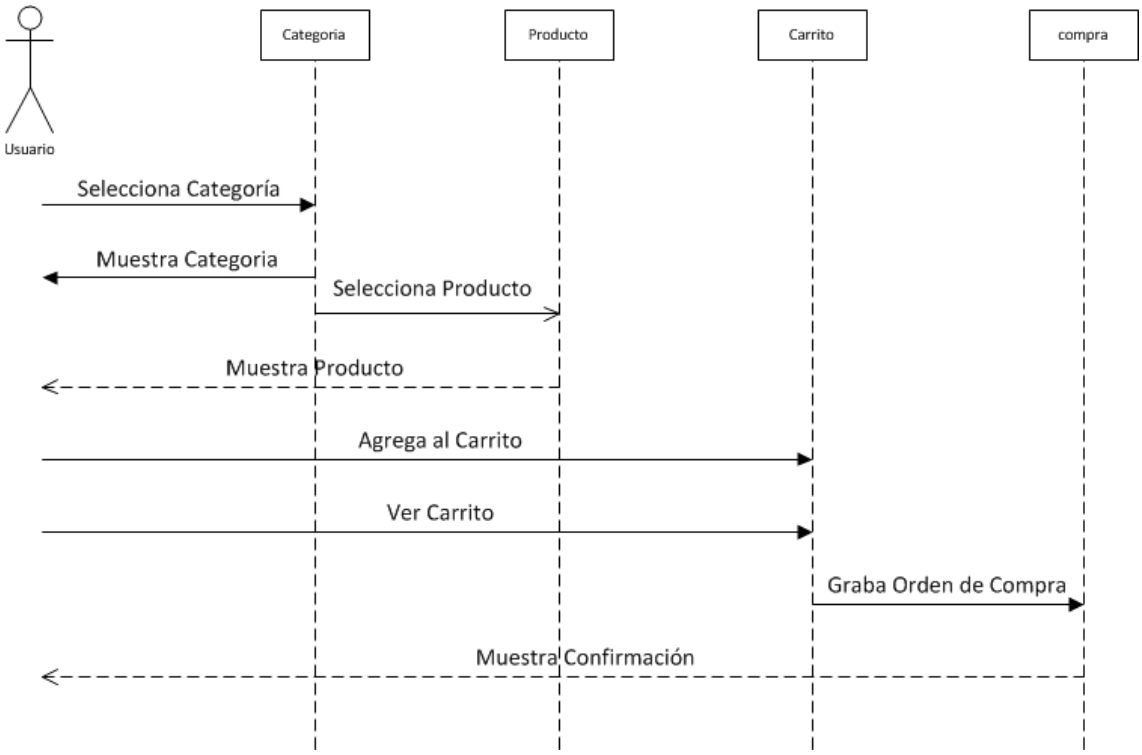


Figura 8. Diagrama de Secuencia. Ingreso Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.4.1.2 Modificar Compra

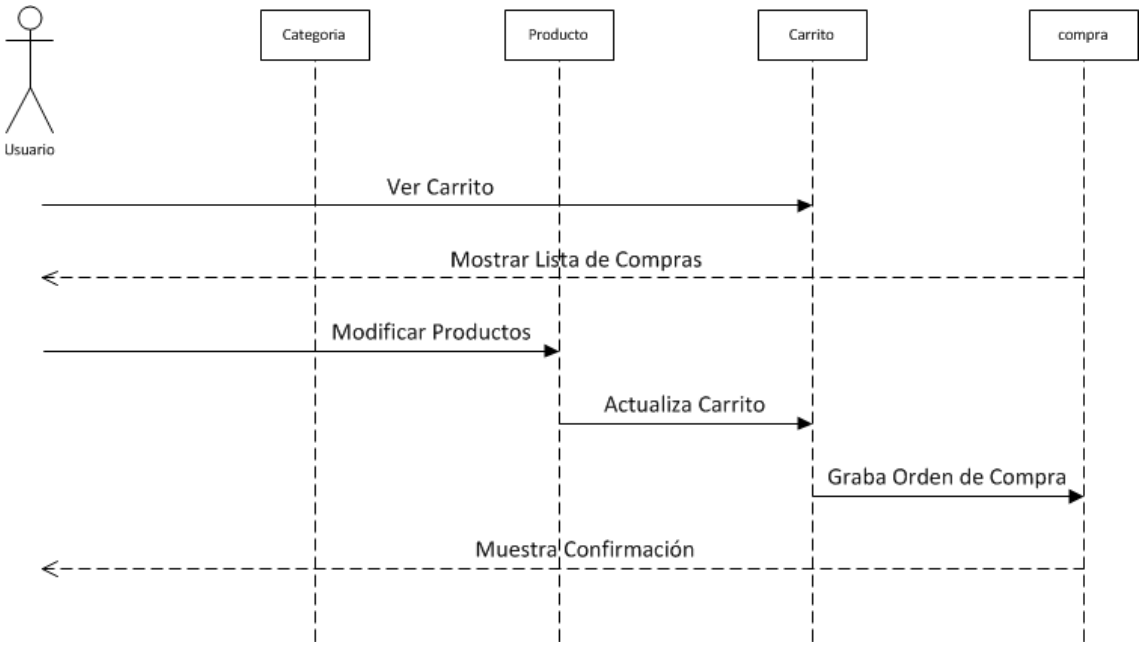


Figura 9. Diagrama de Secuencia. Modificar Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.1.4.1.3 Vaciar Compra

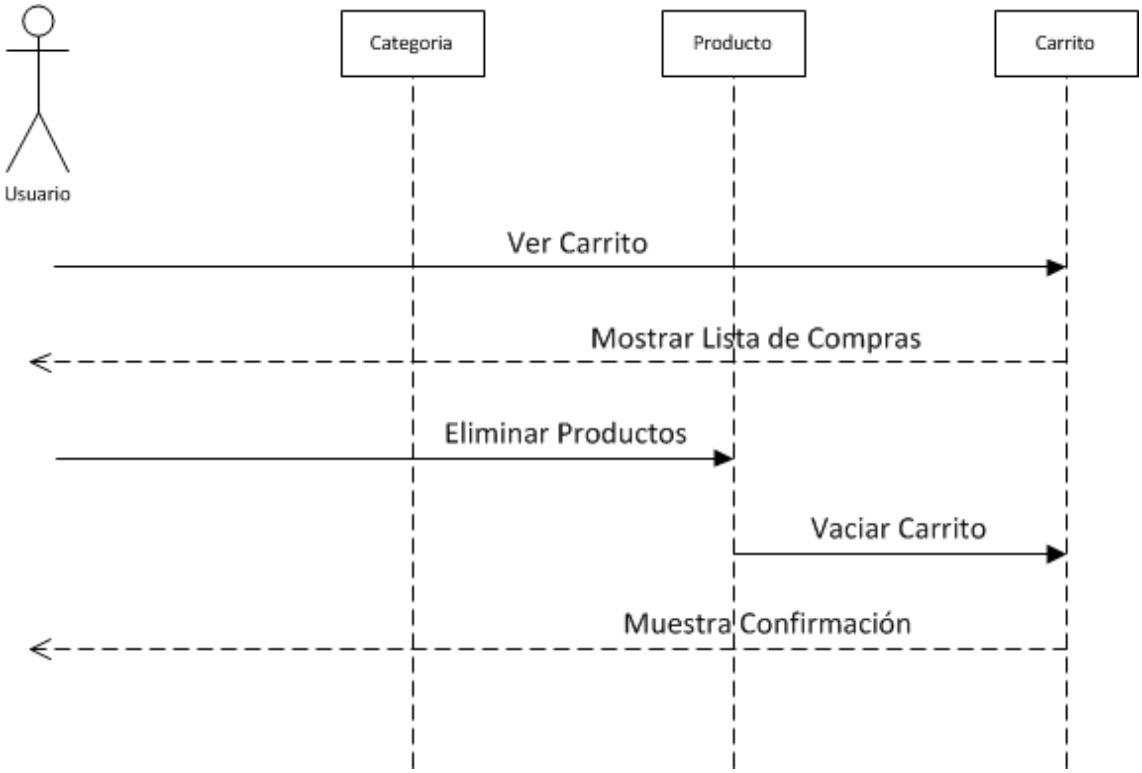


Figura 10. Diagrama de Secuencia. Vaciar Compra (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.2 Diagrama de estructura

Los diagramas de estructura, pueden dividirse en 2 grandes clasificaciones, la primera de ellas son los diagramas de Estructura Compuesta, los mismos que son los que muestran la estructura interna de un clasificador, incluyendo sus puntos de interacción a otras partes del sistema, también modela la configuración y relación de las instancias que juntas determinan el comportamiento del clasificador.

Otra gran clasificación son los diagramas de estructura estática, los cuales muestran el conjunto de clases y objetos que son parte de un sistema, conjuntamente con las relaciones existentes entre éstos, así como también se modela de una manera estática la estructura de información del sistema y la visibilidad que tiene cada una de las clases, dada por sus relaciones con las demás, independientemente del tiempo.

Para el estudio de clases, objetos y relaciones que existen entre ellas, del funcionamiento del carrito de compras, se realiza el análisis en los siguientes diagramas de estructura estática:

2.1.3.2.1 Diagrama de Clases

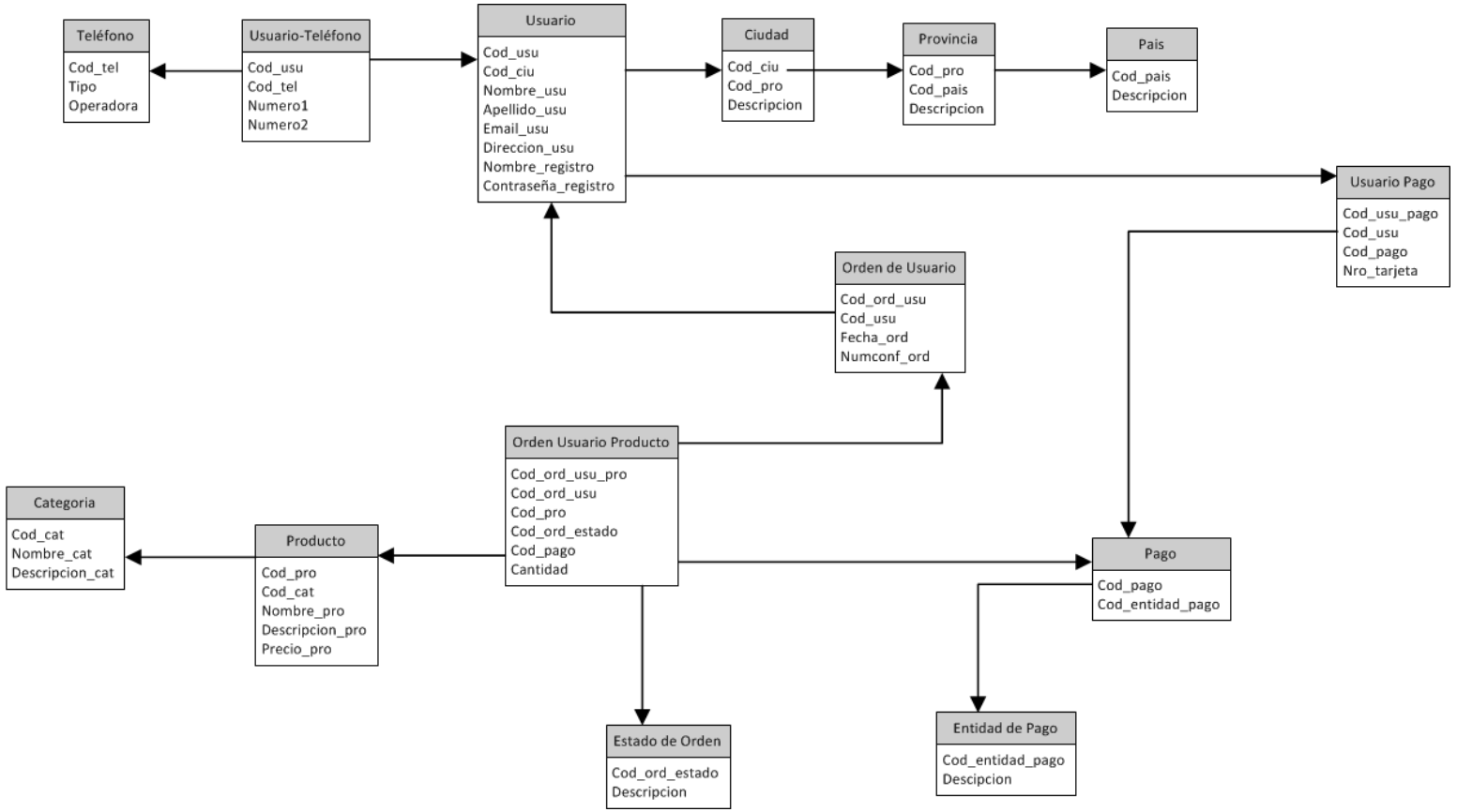


Figura 11. Diagrama de Clases. (Elaboración: Autoras. Cuenca Ecuador 2013)

2.1.3.2.2 Diagrama de Componentes

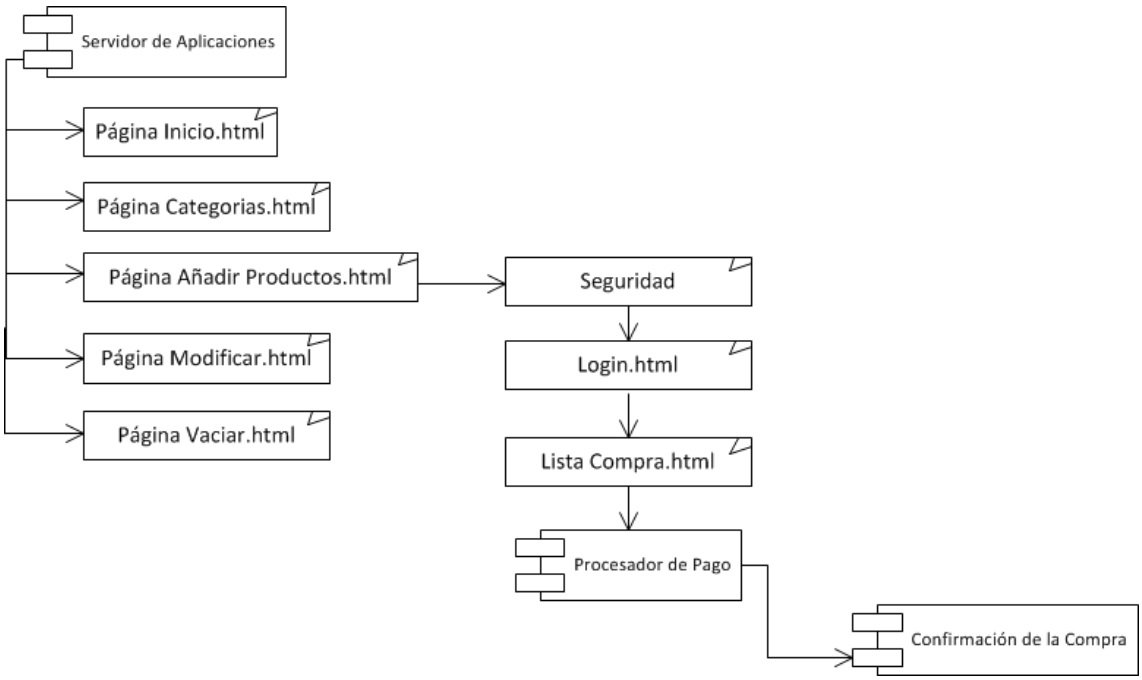


Figura 12. Diagrama de Componentes (Elaboración: Autoras. Cuenca Ecuador 2013).

CAPITULO 3. Seguridad en la implementación del Carrito de Compras

3.1 Definición de seguridad.

El término seguridad proviene de la palabra en latín “securitas” y se define como “la ausencia de riesgo o también a la confianza en algo o alguien”, según la Real Academia de la Lengua Española.

Sin embargo la definición anteriormente mencionada puede tomar diversos sentidos según el área al que se le haga referencia; en este caso se debe hacer énfasis a la seguridad informática, la misma que puntualiza en la investigación y ejecución de políticas de protección de datos en ordenadores por parte de un individuo o equipo de expertos en computación, teniendo como fin la protección de la información y de los mecanismos que ello requieran, mediante diversas prácticas que consisten en la restricción del acceso al sistema o a partes de este, resguardando el funcionamiento del sistema y buscando preservar la integridad de la información, tanto como su confidencialidad, disponibilidad e irrefutabilidad; logrando con esto indicar que dicho sistema está libre de vulnerabilidades; es decir cualquier amenaza, daño, riesgo, ataque, desastre o cualquier situación que pueda afectar a su funcionamiento directo o a los resultados que se obtienen.

Seguridad en las formas de pago

Conscientes de que la tecnología avanza con el tiempo y siendo una necesidad para el mundo entero, existe la posibilidad de comprar mediante la WWW (World Wide Web); la cual utiliza el sistema de pago electrónico para realizar transacciones entre un comprador y un vendedor en línea.

Presentan riesgos que pueden afectar notablemente al desempeño de ésta actividad como por ejemplo los documentos digitales que pueden ser copiados perfectamente una y otra vez, las firmas digitales que corren el riesgo de ser falsificadas por cualquier persona que conozca del medio, teniendo un mayor peligro si es que ésta conociera la clave privada del firmante; puede causar conflicto también si es que la identidad de una persona es asociada equívocamente con la información relacionada en cada pago.

Existen algunas formas de pago entre ellas tenemos TPV-Virtual, Sistemas de Monedero Electrónico, Banca Electrónica del Usuario, entre otras; siendo TPV una de las maneras más seguras para la utilización de tarjetas de crédito mediante Internet, ya que los datos del usuario no serán conocidos de ninguna manera por el vendedor, pues los mismos viajarán de manera encriptada y dicha información conocerá únicamente el banco.

De manera gráfica se explica una compra mediante tarjeta de crédito:

Paso 1

El cliente o usuario entra a la tienda y después de seleccionar los productos que desea comprar, envía el detalle de compra, incluyendo sus datos personales.

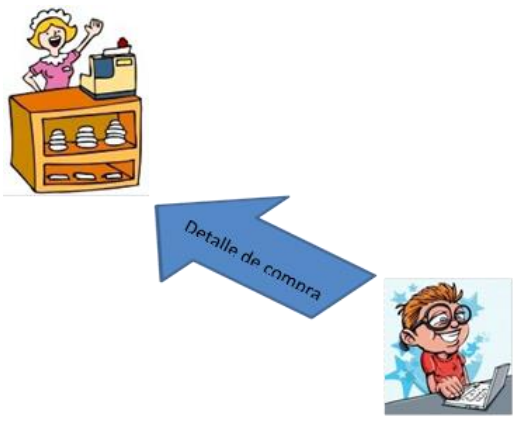


Figura 13. Ingreso del usuario (Elaboración: Autoras. Cuenca Ecuador 2013)

Paso 2

La tienda revisa el detalle de la compra y envía los datos del usuario al banco para la identificación.

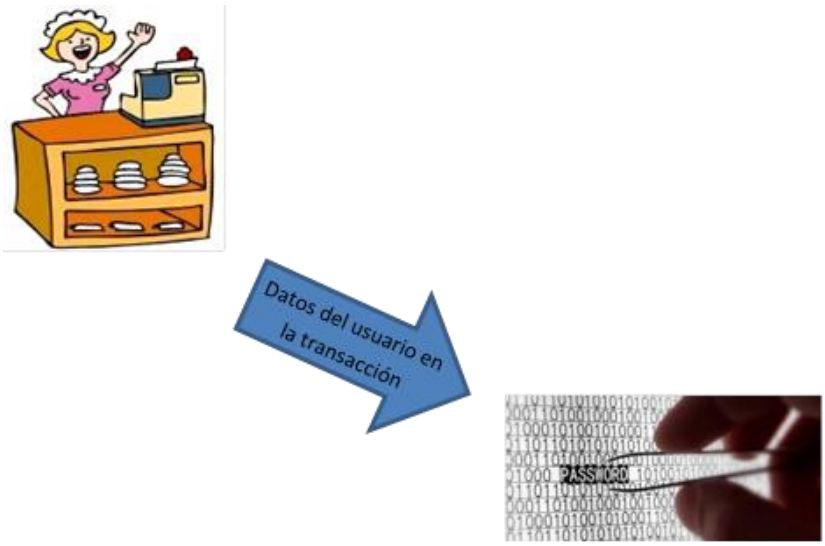


Figura 14. Revisión de la Compra. (Elaboración: Autoras. Cuenca Ecuador 2013)

Paso 3

El banco solicita al cliente información de la tarjeta con la que va a cancelar la compra.

Figura 15. Información de la tarjeta (Elaboración: Autoras. Cuenca Ecuador 2013)

Paso 4

El banco consulta si la información de la tarjeta del cliente es válida.

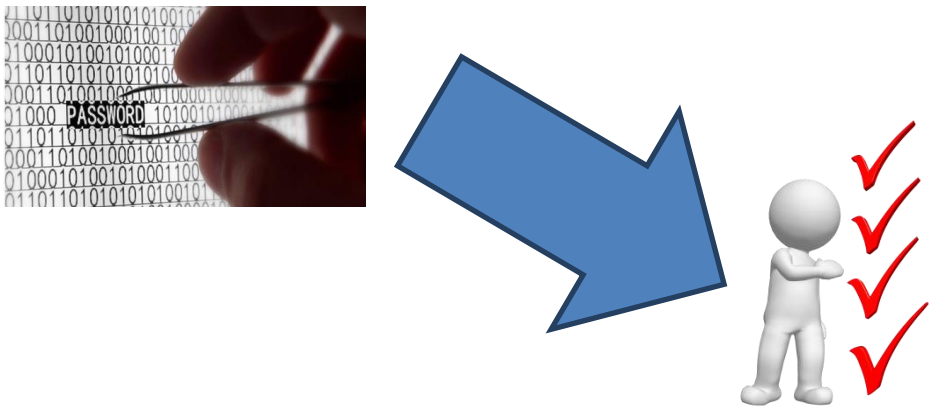


Figura 16. Verificación de la Información. (Elaboración: Autoras. Cuenca Ecuador 2013)

Paso 5

El banco comunica a la tienda y al cliente la conformidad de la operación, así como la cancelación de la cuenta, y el éxito de la compra.

Figura 17. Conformidad de la Operación (Elaboración: Autoras. Cuenca Ecuador 2014).

Para la encriptación de la información se utilizan fórmulas matemáticas y para des encriptar se usa una clave con un parámetro de esas fórmulas. Las técnicas que se

manejan en el cifrado consisten en manipular la información y de este modo conseguir:

- Confidencialidad: Solo puede acceder a la información el destinatario.
- Autentificación: Tanto el emisor con el receptor pueden confirmar la identidad de la otra parte.
- Integridad: La información no puede ser alterada.

Se puede listar algunos métodos de la Criptografía:

- Cifrado simétrico: Utiliza una única clave compartida.
- Cifrado asimétrico: Utiliza claves públicas y privadas.
- Funciones hash: Asocian un número a un documento.
- Cifrado híbrido: Combina cifrado simétrico, cifrado asimétrico y funciones hash.

Como se mencionó anteriormente, otras de las formas de seguridad son las certificaciones y firmas digitales, los mismos que presentan diversos datos como:

- Entidad del titular.
- Su clave pública para la comunicación.
- CA (autoridad de certificación), es un organismo que de acuerdo con unas políticas y algoritmos, certificará claves públicas de usuarios o servidores.
- La firma en sí.

La firma digital se da a conocer en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, donde se relacionan los datos de una persona o de un equipo informático. La firma digital de un documento es el resultado de aplicar un algoritmo matemático, denominado función Hash, la misma que identifica

probabilísticamente un conjunto de información, a su contenido y, seguidamente aplica el algoritmo de firma (emplea una clave privada) al resultado de la operación anterior, de tal manera finaliza generando la firma electrónica o digital.

El PIN (Personal Identification Number), la contraseña, la clave otorgada por el banco o la tienda en línea, se introducen en un formulario pues éstas claves de acceso en la actualidad se utilizan para comprobar la legitimidad del usuario al realizar una transacción.

Por otra parte el TAN (Transaction Authentication Number), número de autentificación de transacción; se encuentra conformado por una lista de códigos que son previamente generados de manera física o distribuidos antes de realizar la transacción de manera digital o mediante dispositivos electrónicos, en todos los casos se solicita una clave nueva para cada transacción. El TAN tiene variantes del sistema, como:

- mTAN: El banco envía el número de identificación antes de la transacción, a través del celular del cliente posiblemente en un mensaje.
- iTAN: Tabla de códigos con índices correspondientes a tarjetas de coordenadas bancarias, es decir se pide introducir la clave correspondiente a la fila X con la columna Y.
- iTANplus: Añade *captcha*, una variante que proporciona números y letras distorsionadas para que un software no pueda reconocer tan fácilmente, ya que estas letras convertidas en frases serán comprendidas solamente por humanos y no por programas automatizados.
- OTP (*One Time Password*) o también llamada contraseña de un solo uso, generalmente se envía una clave a través de correo electrónico o mediante un

mensaje de texto, también puede ser generada mediante los dispositivos *tokens*. Este código deja de ser efectivo cuando la transacción es realizada con éxito.

Los Tokens son dispositivos electrónicos independientes o de conexión USB a una PC, los cuales generan claves privada de manera aleatoria según un patrón o por sincronización mediante un servidor externo; el banco solicita introducir la clave de acceso generada por el token del cliente en un momento dado.

Existen también los teclados virtuales, los cuales no sirven como un sistema de identificación, al contrario es un medio óptimo para introducir las credenciales del usuario generalmente en las webs bancarias, donde se debe introducir la contraseña o las coordenadas. Los teclados virtuales existen dentro del sistema operativo o el software antivirus como un mecanismo de introducción de datos de manera virtual dejando a un lado el teclado físico; siendo el objetivo evitar los keyloggers o los registradores de pulsaciones en el teclado.

3.1.1 Marco Jurídico

El comercio electrónico ha trascendido en lo que a seguridad de las transacciones en línea se refiere, teniendo una relación directa con cada uno de los aspectos competentes, como son los fraudes, propiedad intelectual, patentes, firmas y contratos digitales. Por ello se debe buscar los mejores procedimientos para proteger al usuario que realiza sus transacciones en línea, siendo uno de estos el marco jurídico, el mismo que aumenta el nivel de confianza de los consumidores y cumple debidamente los derechos de los que ofertan los productos o servicios.

Cada uno de los países y estados cuenta con su propio marco legal, el mismo en el que se estipulan diferentes lineamientos, los cuales fueron formados bajo los siguientes parámetros:

- Información previa al contrato
- Plazo de desistimiento y consecuencias del mismo
- Formulario de devolución y excepciones del mismo
- Costes
- Botón de Pago
- Pagos adicionales
- Atención al cliente

En el Ecuador está vigente la Ley de Comercio Electrónico, Mensajería de Datos y Firmas Electrónicas, la misma que fue expedida en abril del 2002. *"El objetivo de esta ley es normar, regularizar y buscar que se controlen la contratación en los ámbitos civiles y mercantiles, ejecutados por el medio del internet, para facilitar las relaciones económicas y de comercio en el Ecuador"*. (Ley de Comercio Electrónico. 2006. Consejo Nacional de Telecomunicaciones. 18 Diciembre 2014). En esta ley constan los reglamentos y leyes vigentes de nuestro país.

3.1.1.1 Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

Mediante Internet y el nuevo sistema de compra y venta electrónica se ha visto necesario normar, regular y controlar estos procesos, mediante una ley especializada que hable de ello. De esta manera conocer que no se puede crear a la deriva una tienda online; pues para ello es necesario saber las normas y leyes que se deben cumplir, para así evitar futuros conflictos.

El negocio virtual se ha convertido en una de las mayores ventajas para los vendedores ya que el trabajo se lo realiza de manera rápida, con facilidad y comodidad para el cliente, pero tiene la desventaja de no causar como primera impresión la seguridad para navegar y comprar de manera inmediata; por lo tanto los siguientes artículos que dicta la de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, estipulados por el Congreso Nacional son de gran ayuda para que los usuarios tengan mayor confianza al momento de dirigirse a una tienda virtual. (Ley de Comercio Electrónico. 2006. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley No. 2002-67. 18 Diciembre 2014).

3.2 Riesgos y la Seguridad

El comercio electrónico estuvo, está y siempre estará amenazado, ya que es un medio de comercialización no seguro, pues al momento de negociar, se lo hace tras una pantalla, desconociendo la persona que está al otro lado; de una manera totalmente diferente a lo que los compradores están acostumbrados, y los riesgos que lo amenazan son potencialmente peligrosos y nefastos, para poder analizarlos, se debe empezar con una definición de riesgo; y, sería la siguiente:

> ¨*Por riesgo se entiende la contingencia de un daño, o sea, la posibilidad de que al obrar se produzca un daño, lo cual significa que el riesgo envuelve una noción de potencialidad referida esencialmente al daño, elemento éste que estructura todo el derecho de la responsabilidad y le otorga a la teoría que lleva su nombre un contenido esencialmente objetivo en el análisis de los hechos y las conductas que traen como consecuencia un perjuicio.*¨ (SARMIENTO, Manuel. Responsabilidad Civil. Universidad de Colombia. 2002.)

Pero para poder contrarrestar estos riesgos y amenazas, y afianzar la confiabilidad del cliente, se debe tener muy en cuenta uno de los factores indispensables dentro del ámbito del comercio electrónico que sin duda alguna es, la seguridad, ya que ningún usuario se arriesgaría a realizar transacciones en sitios no seguros o que no cuenten con las medidas pertinentes, brindando una mayor confidencialidad.

"*Cuando se trata de la seguridad digital, no existe una defensa impenetrable. Pero se puede reducir el riesgo implementando prácticas operativas seguras*" (Robert D. Austin. Harvard Business Review, 2003).

Si bien, en la actualidad la seguridad es cada día más robusta y los riesgos poco a poco pueden ser controlados, se debe tener igual o más cuidado que antes, ya que siempre es un peligro transmitir información a través de medios electrónicos; las pocas amenazas que inundan a los comercios en línea hoy en día, pueden ocasionar pérdidas muy significativas; es por eso la importancia de detectar, prevenir y detener las violaciones a la seguridad informática, como ya lo dijo Robert Austin, estos riesgos, amenazas, problemas, violaciones; con prácticas operativas bien fundamentadas, dará los resultados exitosos y esperados, creando así un ambiente de seguridad en el portal web, ya que la misma es la que connota la viabilidad del comercio electrónico.

3.2.1 Tipos de Riesgos.

El internet como medio único para realizar transacciones en línea, está al alcance de todas las personas; de aquellas que desean realizar compras y ventas de una manera ordenada y adecuada y también de las que están buscando el mínimo movimiento equivocado o la posibilidad más escasa para cometer fraude; es por ello

que está grandiosa red con múltiples ventajas como la rapidez, comodidad, costos bajos porque no necesitan ya pagar arriendo, ni todo lo que conlleva tener un espacio, un negocio físico; trae consigo una serie de problemas, como:

- El internet es un medio público y ya en algunos establecimientos de acceso libre, razón por la cual facilita la transmisión de datos, y el intercambio de los mismos, sin tener mayor control; lo que originaría un problema de Protección de Datos.
- La ventaja de que el Internet nos sirva como medio de comunicación y de publicación de libros, músicas, artículos, programas on line, tiene su parte negativa, pues se da y muy a menudo problemas con la Propiedad Intelectual.
- Otro de los grandes inconvenientes es la doble imposición, pues resulta complicado determinar donde se la realizará; ya que existe problemas de fiscalidad directa como indirecta.

Así como los tres grandes problemas que se enumeraron, existen muchísimos más, pero esos son los de mayor importancia; los mismos que al ser realizados tienen consecuencias dañinas y hoy en día se les nombra como delitos informáticos, los más conocidos son:

- Violación de datos personales.
- Utilizar información falsa.
- Fraudes.
- Música, libros, publicaciones piratas.
- Virus, gusanos, troyanos informáticos.
- Pornografía infantil.

En el libro de Responsabilidad Civil, el Dr. Manuel Sarmiento, expone que a los riesgos se los puede clasificar en 3 grandes grupos, los mismos que serían:

- Riesgo – Provecho
- Riesgo – Creado
- Riesgo – Profesional

Siendo explicado que el Riesgo – Provecho, cuantifica la obligación de remediar con beneficios el daño causado, creando una relación directamente proporcional entre el beneficio y el daño, es decir a mayor daño realizado, mayores beneficios debe efectuar el causante.

El Riesgo – Creado, tiene mucho que ver con la responsabilidad que recae sobre la persona que realiza el acto, cuando éste crea un suceso que es una amenaza para el otro y crea riesgo, se dice que éste es el único culpable de todos los daños y es acusado sin que se dé lugar a investigaciones.

Por último se afirma que el Riesgo – Profesional apunta firmemente a los daños soportados por el trabajador, y a la calidad de vida que le dan como tal en la institución que labora, no siendo aplicado solamente al ámbito laboral, sino también a todas las actividades que éste conlleva.

Existe otra gran clasificación de los Riesgos, son básicamente tres amenazas que tienen fines de lucro por parte de los atacantes, éstos son:

- Malware. Conocido también como código malicioso y malintencionado, se dedica en gran parte a robar información anidada en los computadores que ya han sido contagiados.

Los códigos maliciosos sustraen información usualmente a través de spyware (aplicaciones que recopilan información del usuario, sin el consentimiento de éste), o de virus que tienen la misma función como los gusanos o troyanos, los mismos que son diseñados para introducir los equipos en redes zombis (botnets) y que así el atacante pueda controlarlas remotamente y realizar sin mayor inconveniente el fraude.

- Phishing. Otra forma de robar información personal, claves y contraseñas, afectando de manera significativa el e-commerce, son los ataques de phishing. Los mismos que se realizan a través de correos electrónicos, mensajes instantáneos, llamadas telefónicas; simulando ser entidades de confianza y así obtener información sensible y privada del usuario.

Tanto en el phishing como en el malware, son riesgos bastante perjudiciales, pues hacen referencia al robo de credenciales que sirvan como acceso a portales web, con el objetivo de utilizarlos de forma indebida, realizando así actividades ilícitas, en la mayoría de casos relacionados con fraudes económicos.

- Scam. Es la acción de realizar estafas, a través de páginas web que contienen información inventada, o de la creación de perfiles falsos para comercializar productos que no existen, mostrar historias conmovedoras o "informar" la ganancia de algún "premio", siempre con propósitos maliciosos, intentando engañar al usuario y teniendo como único objetivo de robar información personal.

En la actualidad son muy comunes los fraudes realizados en línea, es por eso que el usuario debe tener mayor cuidado y comprar a través de comercios electrónicos seguros, pues como lo dijo Bortnik: "*es importante que, para estar seguro ante este*

tipo de amenazas, el usuario cuente con una solución con capacidades proactivas de detección de códigos maliciosos, y adopte ciertas buenas prácticas básicas de seguridad". (Sebastián Bortnik, Gerente de Educación & Servicios de ESET Latinoamérica. 2012)

3.3 Seguridad del PIN

Los fraudes electrónicos tienen una proporcionalidad totalmente directa al crecimiento del e-commerce, pues mientras mayor crece éste último, existen más cantidad de delitos informáticos, ésta es la mayor razón por lo que las casas emisoras de tarjetas de crédito (Visa, MasterCard, Diners, PayPal) buscan, analizan y diseñan medidas de seguridad para intentar minimizarlos, siendo una de éstas la creación de los códigos de seguridad, que tiene como objetivo autenticar al usuario; es decir, confirmar su identidad, saber si la persona que está utilizando es realmente el dueño de la tarjeta.

Estos códigos de seguridad para compras en internet fueron creados para evitar fraudes electrónicos, sin embargo, aún no son muy conocidos por los usuarios; pero con el pasar del tiempo la implementación de ésta capa de seguridad (acción de solicitar el código de seguridad), al momento de presionar el botón de pago en la web será un proceso "normal" y que todos los usuarios deberán seguir para completar su transacción en línea.

Este protocolo de seguridad fue iniciado por Visa, el mismo que lo denominaron "3-D Secure", pero que ya desde hace algún tiempo las principales tarjetas lo crearon para compras en Internet, conocidos de la siguiente manera: en MasterCard como SecureCode (SC), en Diners Club como Payclub (PC) y en Visa actualmente se lo conoce como Verified by Visa (VbV).

Este código de seguridad denominado PIN (número de identificación personal) es utilizado para verificar el titular de la tarjeta en el momento de la transacción. Que puede tener varios dígitos, entre los cuales constarán, números, letras, o ambos; es una clave utilizada para verificar al titular de la tarjeta en el momento de la transacción; es decir la identidad del titular de la misma se encuentra exclusivamente oculta en el PIN, el cual es creado por el usuario, y será solicitado cada vez que éste proceda a realizar el pago en la web.

En caso de que el usuario nunca ha creado su código de seguridad, al momento de ingresar los datos para realizar el pago correspondiente, éste lo detecta y automáticamente en la misma sesión de pago lo hace pasar por el proceso de la creación del código, y dependiendo del banco emisor, pedirá datos como el número de cédula, CVV, fecha de caducidad de la tarjeta, etc.; con el único fin de autenticar al tarjetahabiente.

El portal electrónico debe cumplir un conjunto de requisitos de seguridad reconocidos, para garantizar la confidencialidad del PIN del tarjetahabiente; dándole mayor seguridad al cliente, pues el PIN tiene protección criptográfica de su identidad, la misma que requiere la implementación de controles específicos para asegurar su nivel de seguridad, éstos requisitos son alineados a nivel internacional para la protección de los datos.

El incumplimiento de estos controles y requisitos específicos aumenta el riesgo de fraude para los tarjetahabientes, ya que no solo producirían pérdidas en dólares tangibles para éstos; sino también para los negocios que tendrían que corregir e investigar dichas acciones fraudulentas, a parte de la desconfianza y mala reputación que ganaría cierto comercio electrónico.

Los programas de seguridad PIN con los que cuentan cada una de las instituciones antes mencionadas, están comprometidos para brindar el máximo nivel de protección para los titulares de tarjetas durante la transmisión y el procesamiento de transacciones.

Cuando un comercio electrónico cumple los requisitos de seguridad del PIN aumenta la confianza para los comerciantes, instituciones financieras y los usuarios, manteniendo así la integridad de un entorno seguro de procesamiento de pagos.

3.3.1 Requisitos del PIN

Garantizar la confidencialidad de PIN del tarjetahabiente requiere que el portal electrónico cumpla con un conjunto de requisitos de seguridad reconocidos, los mismos que se encuentran divididos por objetivos, siendo los siguientes:

3.3.1.1 Objetivo 1.

"*Los PIN utilizados en operaciones reguladas, tienen requisitos que se procesan utilizando equipos y metodologías que afirmen mantenerse seguro*" (Visa PIN Security Requirements Auditor's Guide. 2002. Visa. 10 Diciembre 2013), los requerimientos que debe cumplir el e-commerce en éste objetivo serían:

- Todo tarjetahabiente debe contar con un código PIN, el mismo que deberá ser procesado con equipos que aseguren su criptografía, es decir dispositivos (SCD), estos dispositivos son muy sensibles y seguros, pues una vez ingresada la información al SCD, causa inmediata borrada de los PINs, su criptografía, llaves, teclas y toda información útil que pueda prestarse para fraudes.

- El titular de la tarjeta PIN será procesado en conformidad con las **Normas Internacional/ Industria** aprobadas, para el caso de estudio las más importantes son:
    - El PIN on line sólo debe producirse mediante uno de los métodos de gestión de claves permitidas: DUKPT, llave fija, llave maestra / sesión clave
    - El PIN on line debe ser cifrado mediante un algoritmo y el tamaño de la clave se debe especificar en la norma ISO 9564. Éste algoritmo es el único aprobado en la actualidad para otorgar PINs en línea según lo descrito en la norma ANSI X9.52.
- La información de todo titular de la tarjeta que tenga tecnología PIN, otorgada en línea; debe estar cifrada con una técnica criptográfica probada, que proporcione un nivel máximo de protección y que sea compatible con las normas internacionales de seguridad.
- Las tarjetas deben ser protegidas de acuerdo con los requisitos establecidos en el Libro EMV IC Card Specifications for Payment Systems, existen dos métodos sobresalientes, que son:
    - **Bloque de PIN Cifrado.** Se presentará una tarjeta con microprocesador “IC” cifrada con una clave autenticada de la IC.
    - **Bloque de PIN de texto plano.** No se encriptará el PIN, pues se requiere el bloqueo del mismo, que será cifrado con un Lector de circuito integrado de acuerdo con la norma ISO 9564.
- Para la transmisión segura del PIN desde el emisor de la tarjeta, éste debe estar en un formato bloque de PIN encriptado, el mismo que cumplirá la norma ISO 9564 Formato 0, 1, o 3.

Para ello es necesario recordar que el PIN puede ser de cualquier longitud que vaya de 4 a 6 caracteres; y el tamaño del campo del bloque de PIN cifrado es un fijo de 16 caracteres de longitud. Por lo tanto, el PIN cifrado es combinado con otros datos para llenar completamente este campo, teniendo en cuenta las variaciones de los Formatos 0, 1 y 3 de la ISO 9564

- Las transacciones basadas en PIN deben tener lugar en tiempo real, es decir en el proceso normal que sufre el mismo, el que sería el siguiente: PIN introducido por el titular de la tarjeta, luego el cifrado y encapsulado en un mensaje del mismo y por último transmitido a la entidad autorizante que toma la decisión de aprobación o negación del PIN. Luego de éste proceso el PIN debería ser eliminado para asegurarlo, salvo algunos casos en los que se requiere que el mismo sea almacenado, como por ejemplo con el fin de recuperar el procesamiento de autorización, almacenamiento de otros elementos de datos, etc.; según lo señalado en la ISO 9564, pero debe serlo con la mayor seguridad del caso, es decir guardado bajo una clave de cifrado diferente a la que se utilizó en la transacción y por un tiempo mínimo.

3.3.1.2 Objetivo 2.

"Las claves criptográficas utilizadas para el cifrado, descifrado de PIN y gestión de claves relacionadas, son creadas utilizando procesos que aseguren que no será posible predecir o determinar cualquier llave" (Visa PIN Security Requirements Auditor's Guide. 2002. Visa. 10 Diciembre 2013).

- Todas las claves y sus componentes deben ser generados de tal manera que sea imposible determinarlas, con procedimientos de generación de números aleatorios o pseudo-aleatorios, teniendo en cuenta que ésta creación debe

basarse en estándares de buena calidad, generados obviamente aleatoriamente.

- El proceso de generación de la clave debe ser controlado por al menos dos personas autorizadas que pueden asegurar que no hay un tercero no delegado o algún mecanismo capaz de revelar un componente de clave secreto o privado de texto sin cifrar. Cualquier residuo que se encuentre del proceso de impresión, exportación, visualización o grabación que pueda revelar un componente o clave, debe ser destruido antes de que una persona no autorizada puede obtenerlo.
- Los procedimientos de generación de llaves deben ser documentados, así como también debe permanecer escrito la responsabilidad de cada uno de los custodios de claves, el personal de supervisión, gestión técnica, etc.

3.3.1.3 Objetivo 3.

"Las claves son transmitidas de una manera segura" (Visa PIN Security Requirements Auditor's Guide. 2002. Visa. 10 Diciembre 2013).

- Las claves públicas y privadas deben ser transmitidas de tal manera que se proteja su integridad y autenticidad
    - El objetivo de éste requerimiento con respecto a la clave criptográfica privada es que al momento de enviarla de un lugar a otro, permanezca totalmente secreta, para ello se suele utilizar el mecanismo que envía la clave dividida, y la transmite a 2 personas que tendrán parte del conocimiento, pero no lo suficiente para comprometer la llave.
    - Cuando una clave criptográfica pública se envía de un lugar a otro, de debe usar algún mecanismo independiente que tenga la capacidad de

validar que se ha recibido la llave correcta, usualmente se la envía mediante un texto cifrado.

- Todos las claves cifradas que se van a transmitir deben contener otra clave o encriptación tan fuerte como cualquier llave transportada.
- Los procedimientos de transmisión y transporte de claves deben estar documentados, y en éstos deben constar todas las partes encargadas de dichos procedimientos, así como los eventos de transmisión de la misma.

3.3.1.4 Objetivo 4.

"Las claves son usadas de una manera que previene o detecta su uso no autorizado" (Visa PIN Security Requirements Auditor's Guide. 2002. Visa. 10 Diciembre 2013).

- Cuando se comparte una clave entre dos organizaciones (portal-tarjetahabiente, portal-entidad financiera) se debe utilizar la técnica definida como "Zona de Cifrado", es decir utilizar claves cifradas y no otorgar a ningún tercero.
- Debe existir procedimientos que eviten o detecten las llaves no autorizadas y/o el reemplazo y mal uso de éstas, se encuentren o no cifradas. Esto reducirá el riesgo de que un adversario sustituya una clave, con caracteres conocidos para él.

  Estos procedimientos deben incluir la investigación de varios errores de sincronización y para evitarlos se debe prestar especial atención a la documentación de éstos componentes clave que muestren signos de deterioro, pues darán lugar al descarte y la invalidación de los componentes y de todos los lugares donde se encuentre asociada la clave.

- Los diagramas de encriptación de claves deben ser utilizados con ese único propósito y jamás ser compartidos entre producción y sistemas de prueba, con el único objetivo de limitar la magnitud de la exposición de las mismas.

  Las claves nunca se deben compartir, es decir las empleadas en la producción nunca debe ser utilizados en las pruebas y viceversa.

3.3.1.5 Objetivo 5.

"Las claves se administran de una manera segura" (Visa PIN Security Requirements Auditor's Guide. 2002. Visa. 10 Diciembre 2013).

- Una aplicación que contenga o tenga acceso a los componentes claves, debe tener un contenedor físico de bloqueo seguro, evitando así que personas no autorizadas tengan acceso a dicha información
- Debe existir procedimientos para reemplazo por sospecha de robo de contraseña, los mismos que deben tener documentación y ser notificados a las organizaciones que usan la clave.

  Los procedimientos deben incluir una evaluación de los daños y las medidas específicas que deben adoptarse con el software del sistema y en lo referente al hardware, lo que son las claves y datos de cifrado.

  La documentación debe incluir la sustitución y destrucción de esa llave y todas las variantes y transformaciones irreversibles de la misma.
- Una clave utilizada para proteger el cifrado del PIN nunca debe ser empleada para ningún otro propósito criptográfico.
- Las claves y componentes de las mismas que no son utilizados o han sido reemplazados de forma segura, deberán ser destruidos; los procedimientos para la destrucción de dichas claves deben estar documentados.

- Se debe limitar el número de custodios de claves, es decir designar un solo custodio a cada componente, ésta designación debe ser documentada y él mismo debe firmar un formulario de Custodio Key, los que autorizan e identifican las responsabilidades de salvaguardar componentes claves u otros materiales de claves que se les confía.

  Cada custodio tendrá un tutor, quien debe firmar un formulario de CustodioClave, en el que se reconoce sus responsabilidades para con el custodio, las claves y su componentes.
- Las claves serán almacenadas en componentes físicos, los mismos que deberán guardar registros de las personas que tienen acceso, así como de la fecha, hora de entrada / salida del acceso, nombre y firma del responsable.

3.3.1.6 Objetivo 6.

"El equipo utilizado para procesar los PIN y las claves se gestiona de una forma segura" (Visa PIN Security Requirements Auditor's Guide. 2002. Visa. 10 Diciembre 2013).

- El hardware que se utiliza para el procesamiento del PIN (por ejemplo, PED y HSM) deben ser gestionados y colocados, solo si existe garantía de que él mismo no ha sido manipulado sin autorización, recordando que deben existir controles para proteger los dispositivos criptográficos antes, durante, y después de la instalación; así como también la documentación definida y controlada del acceso a éste hardware.
- Si un equipo ha sido retirado de servicio, todas las claves almacenadas dentro de éste dispositivo criptográfico deben ser destruidas.

- Deben existir procedimientos escritos donde se registren todas las pruebas e inspecciones dadas a los dispositivos PIN de procesamiento antes de ser puestos en servicio.

3.3.2 Administración del PIN

En la actualidad la mayoría de las personas dependen en gran medida de sus tarjetas de crédito para acceder a dinero en efectivo o realizar compras on line, los mismos que se manejan con un código PIN, como se manifestó en el tema anterior; para ello es necesario conocer la forma en la que se genera, modifica, elimina el PIN.

3.3.3 Generación del PIN

Este proceso debería realizarlo el titular de la tarjeta, pero puede existir casos donde alguien de confianza pueda ejecutarlo; para ello debe tener claro que el código escogido contendrá al menos cuatro dígitos numéricos, y será lo suficientemente grande como para asegurar que la probabilidad de adivinarlo sea nulo, pues el número de intentos posible son mínimos.

La generación del PIN, se puede realizar de tres maneras básicamente:

- **PIN Asignado** Este proceso se realiza cuando el emisor designa un PIN que se genera usando un algoritmo de cifrado con una longitud de clave apropiada según normas existentes en la ISO TR 14742.
- **PIN Asignado al azar:** Creado mediante un número aleatorio, para ello se utiliza un generador que sea compatible y que cumpla todos los lineamientos de la norma ISO / IEC 18031, cabe recalcar que el mismo deberá ser aprobado por la NIST SP 800 - 22.

- **PIN Seleccionado:** El Titular de la Tarjeta seleccionará su PIN usando como guía los lineamientos de la norma ISO 9564, algunas de ellas que se deben tomar en cuenta son:
    - Los bancos deben informar a los titulares de tarjetas contra el uso del PIN como credencial para banca a distancia o cualquier otro servicio.
    - Procurar utilizar un formato alternativo para las credenciales de banca a distancia, por ejemplo no colocar números.
    - El titular de la tarjeta debe tener orientación permanente y adecuada para la selección del PIN y su uso.

3.3.3.1 Selección del PIN por correo electrónico

- Dar instrucciones inequívocas para completar el formulario.
- Utilizar un número de referencia criptográfico para enlazar el PIN seleccionado con su cuenta.
- Utilizar una referencia que no comprometa, y sea muy diferente al número de cuenta.
- En el formulario no escribir ninguna información que se relacione directamente al PIN como el nombre, dirección o teléfono del titular de cuenta.
- Las claves criptográficas utilizadas para generar o proteger los números de referencia deben ser manejados de acuerdo a los procedimientos de gestión de claves, que cada institución maneje.
- El personal emisor de estos procesos no debe tener acceso directo que permita la manipulación de texto del PIN.

- Los únicos que deben tener acceso a datos concretos del tarjetahabiente y vincularlos con su cuenta, será el personal autorizado.
- Cualquier papel o residuo que contenga información que comprometa a la clave PIN debe ser destruido.

3.3.3.2 Selección del PIN por Internet

- El titular de la tarjeta que se comunique, recibirá un asesoramiento en el sistema de notificación del PIN vía internet.
- El proceso de selección del PIN por Internet contiene algoritmos de protección criptográfica para asegurar la transmisión del PIN durante la transacción de procesamiento, hasta llegar a la computadora del titular de la tarjeta.
- La selección de PIN por Internet requiere de instrucciones que el titular de la tarjeta debe seguir, como por ejemplo brindar información preestablecida, la misma puede ser el número de control, el valor del PIN elegido y los datos de autenticación.
    - Los valores del número de control y autenticación no deben revelar números de cuenta.
    - El número de control debe ser generado y transmitido al titular de la tarjeta mediante un correo electrónico, con ello lograremos que solo el tarjetahabiente puede obtener su número de control.
- Cualquier clave criptográfica utilizada para generar un número de control no debe tener ningún otro fin y debe ser manejado de acuerdo a la norma ISO 11568.

- El sistema no debe tener ningún procedimiento que permita asociar un número de control o valores de autenticación con el nombre, números de teléfono, dirección o números de cuenta del titular de la tarjeta asociada.
- El sistema de selección de PIN asocia el número de control con un valor específico, validando así los datos del titular de la tarjeta y recuperando el código PIN del mismo, para así poder realizar la transacción.
- El número de control y la clave PIN no convienen registrarse, éstos deben suprimirse inmediatamente después de su uso.
- El sistema de selección de PIN debe ser diseñado y operado con procedimientos estrictos, y encapsulados, de manera que ninguna persona sea capaz de asociar el número de control, clave PIN o autenticación con un número de cuenta específico.
- La seguridad de la aplicación de selección PIN se basa en una premisa, la misma que afirma que ningún individuo podrá asociar un número de control con una cuenta específica.
- El procedimiento que permite la selección de PIN por Internet debe estar protegido, y transmitirse mediante un canal seguro establecido entre la aplicación cliente en el PC del usuario y el servidor, según lo que dicta la norma ISO / IEC 11770.
- La aplicación debe tener en cuenta los ataques MITB.

3.3.3.3 Autenticación del PIN

- El emisor se asegurará de que al asociar la autenticación del titular de la tarjeta, con el número de control; éste no debilitará el principio que dicta

los lineamientos de que el número de control no se utilice para determinar una cuenta específica.

- La autenticación del titular de la tarjeta no debe ser realizada por el servidor de Internet, al contrario debe ser formalizada por el sistema host emisor y sólo si es que el número de control se logró asociar a una cuenta específica.
- La autenticación del titular de la tarjeta y la generación del PIN de referencia deben ser realizados en tiempo real, y el éxito o fracaso reportados al titular.
- Los servidores Web deben estar configurados para deshabilitar el caché del cliente web.

3.3.3.4 Autenticación del PIN mediante un Sistema de Gestión

- Los emisores que permiten a los titulares de tarjetas administrar remotamente su PIN a través de Internet, pueden autenticarlos proporcionando credenciales para un sistema denominado gestión de PIN.
- El titular de la tarjeta que desee acceso a su PIN, o a la modificación del mismo deberá utilizar un mecanismo de autenticación de alta seguridad.
- La aplicación que conlleva éste proceso, debe asegurar que éstas actividades se pueden hacer de una manera que reduce al mínimo el riesgo de exposición del PIN y los datos de cuenta asociadas.
- Debe haber un procedimiento que permita a los tarjetahabientes contar con un medio que determine que el diálogo que realice con el emisor es genuino.

- Las credenciales de autenticación del titular no deben basarse en información que esté disponible a terceros.
- El único requisito para autenticar a un titular de la tarjeta no debe ser solo el PIN generado en el sistema, sino también información de la tarjeta y de su dueño.
- Las preguntas que se realizan los titulares de las tarjetas para confirmar su identidad, no deben ser las mismas; es decir deben variar cada vez que el titular de la tarjeta accede al sistema.
- Los emisores deben evitar el uso de la clave PIN como una credencial para realizar las transacciones de pago, acceso, cambio de clave, etc.
- El emisor debe evitar el envío de peticiones de administración no solicitados del PIN a sus usuarios.
- En caso de que el cliente desee el servicio a través de una línea telefónica, debe tener en cuenta las siguientes medidas:
    - La identificación de la línea de llamada entrante (CLI) no debe utilizarse como único medio de autenticación del titular.
    - El CLI es vulnerable a la suplantación de identificador de llamadas, por eso puede ser utilizado solo como una confirmación para verificar la identidad del titular de la tarjeta, pero no como una prueba.
    - Si el titular de la tarjeta se pone en contacto vía telefónica con un número ya que se había registrado, la persona que contesta el teléfono de la entidad emisora, no se debe asumir que es el titular de la tarjeta.

- A los titulares de tarjetas que requieren la transmisión de la clave PIN a través de redes abiertas se les debe ofrecer garantías de que el PIN sólo se entrega al tarjetahabiente.

3.3.3.5 Transmisión del PIN

- El objetivo principal de éste proceso es, que el PIN y los datos de las cuentas asociadas que sean transmitidos desde un sistema a otro deben ser protegidos contra la divulgación, protección de la integridad, o posibles manipulaciones
- Uno de los aspectos que requieren mayor atención, es la integridad del PIN, la misma que se refiere a cuidar la relación entre el valor del PIN y cualquier información asociada, como los datos de la cuenta del usuario y la información de sus transacciones.
- Las principales amenazas en la transmisión son :
    - Dependencia de cifrado de red (que no se utilice una técnica de cifrado comprometida, donde la aplicación esté bajo control.).
    - Los ataques contra los algoritmos criptográficos utilizados para cifrar los códigos PIN y proporcionar la integridad al mismo.
- El número PIN debe ser protegido durante la transmisión por uno o más de los siguientes procesos:
    - Prestación de protección física
    - Codificación del valor del PIN
    - La separación del PIN con el número de control.
    - Los protocolos de transmisión del PIN deben ser diseñados de tal manera que la introducción de mensajes fraudulentos, o la

modificación de mensajes válidos, no produzcan ninguna información útil con respecto al PIN.

- La transmisión del PIN y sus datos asociados deben contener procedimientos de cifrado.

- El método utilizado para dar formato a un bloque de PIN antes de su encriptación, no debe permitir que el texto cifrado sea recuperado.
- Cualquier algoritmo criptográfico utilizado para la protección de la transmisión del PIN, debe tener un nivel de seguridad adecuado a la tarea. Esto debe ser evaluado de acuerdo a los convenios, protocolos y los estándares de la industria según su norma ISO 11568.
- Las transmisiones PIN sin cifrar, no deberían contener ninguna información que se puede conectar directamente con el titular de la tarjeta o de la cuenta.
- La transmisión del PIN sin cifrar debe proporcionar integridad y seguridad.

3.3.3.6 Registro del PIN

- El registro de las transacciones que contienen PIN deben ser evitados, pero si es necesario se debe cumplir lo siguiente:
  - El PIN no debe estar a la vista de un tercero.
  - El registro del PIN y / o bloqueo del mismo, no se conservará durante más tiempo de lo necesario para completar la transacción

- Los reclamos relacionados a la divulgación de información del titular de la tarjeta PIN y / o fraude se registran como posible fuente de fallo o mal uso.

3.3.3.7 Almacenamiento del PIN

- El almacenamiento del PIN y los datos de las cuentas asociadas deben ser mínimos, y en lugares necesarios para un funcionamiento fiable de los sistemas.
- Si es necesario almacenar el PIN, se lo debe realizar de manera que no haya personal emisor o un tercero que logre obtener información secreta relativa al mismo.
- Un PIN almacenado sólo se puede cambiar por el emisor o el titular de la tarjeta bajo autorización.
- No se recomienda almacenar el PIN, si las operaciones fiables se pueden lograr sin realizar éste proceso.
- El almacenamiento en vano, incentiva a los hackers a obtener acceso a los sistemas internos que almacenan los PIN y los datos asociados a éste.
- Los datos asociados, el PIN, y / o las claves secretas utilizadas para protegerlo, deben almacenarse en lugares donde su integridad y confidencialidad puedan ser protegidos al cien por ciento.
- El PIN debe ser almacenado dentro de los sistemas del emisor utilizando uno de los siguientes métodos:
    - Como un objeto de datos encriptados, utilizando un algoritmo de cifrado estándar y claves.

    - Como un objeto de datos encriptados, con algoritmos distintos a cualquier otra técnica de cifrado de información.
- Los algoritmos de cifrado de PIN para el almacenamiento de los mismos, deben basarse en los lineamientos de la norma ISO 9564.
- El cifrado del PIN almacenado debe incorporar datos como el número de cuenta, etc., para así verificar y evitar la sustitución de algún valor para ser reemplazado en el proceso de almacenamiento.
- Todos los dispositivos utilizados para almacenar PIN deben ser diseñados y manejados de tal manera que la información no se pueda determinar mediante la manipulación de diferentes entradas en el dispositivo.
- Las instituciones emisoras de las tarjetas de crédito, deben ser sometidas a un proceso de auditoría, donde se revise todos los aspectos del diseño lógico y físico, así como los procesos de almacenamiento de PIN, la gestión de claves, las políticas y procedimientos de los mismos.
- Las instituciones emisoras deben realizar procedimientos y establecer políticas de investigación de antecedentes de pre-empleo para el personal dedicado a las operaciones de almacenamiento y procesamiento del PIN.
- Durante el proceso de almacenamiento, todas las operaciones pertinentes a seguridad deben ser cumplidos bajo control dual.
- El PIN no puede ser almacenado en la banda magnética de una tarjeta.

3.3.3.8 Procesamiento del PIN

- Una de las mayores amenazas en el procesamiento del PIN, son los delincuentes, quienes obtienen acceso a los finales de los procesos del sistema, donde se lleva a cabo la verificación del PIN y el acceso a:
    - Los PIN y los datos asociados durante el almacenamiento.
    - Los PIN y los datos asociados durante la transmisión
    - Los PIN y los datos asociados durante el procesamiento
    - Los códigos PIN deben ser protegidos durante todo su procesamiento, mediante:
        - Protección física
        - El uso de sitios e historiales.
        - Codificación del valor PIN mediante algoritmos apropiados y sus longitudes de clave.
        - Separación del PIN con relación a los datos de la cuenta.
- Un dispositivo que procesa información del PIN, o relacionada al mismo debe ser más que un componente físico, es decir, debe:
    - Proteger el intercambio de datos por medios físicos o por medios criptográficos.
    - Usar un componente que a pesar del envío de uno o más mensajes fraudulentos, no brinden ninguna información útil con respecto a un PIN.

3.3.3.9 Verificación del PIN

- La verificación del PIN en línea, será únicamente la responsabilidad del emisor y deberá ser realizado por éste o por un proveedor de servicios designado.
- El proceso de verificación del PIN on line, implica que éste deberá ser suministrado por el titular de la tarjeta y éste proceso será realizado únicamente por el emisor en un dispositivo denominado HSM.
- Los emisores deben bloquear una cuenta después de que el PIN sea intentado ingresar erróneamente por 3 veces consecutivas, tras lo cual el titular de la tarjeta debe ponerse en contacto con el emisor o su agente.
- Los emisores deben investigar los motivos por los que los usuarios tienen fallas en la verificación de una cuenta, y los cuales no han sido cometidos consecutivamente.

3.3.3.10 Cambio del PIN

- Los valores del PIN y sus detalles sólo deben ser visibles para el asociado titular y por lo tanto modificados por él.
- El cliente debe tener mucho cuidado en la clave que modifica, pues puede seleccionar un valor de PIN que sea fácil de adivinar.
- El cambio de PIN del tarjetahabiente puede realizarse utilizando cualquier dispositivo emisor que sea aprobado y previamente probado su funcionalidad.
- El cambio de PIN debe seguir los principios y lineamientos establecidos en la norma ISO-9564.

- Bajo ninguna circunstancia el cambio de PIN debe realizarse por correo electrónico.
- El cambio de PIN debe ser manejado de manera diferente del de un PIN olvidado, y no se lo debe realizar mediante una interfaz humana intermedia.
- Los cambios de PIN deben quedar registrados para la futura resolución de disputas.
- Una de las pruebas más comunes utilizadas para identificar al titular de la tarjeta es, si éste conoce el PIN actual.
- El cambio de PIN en línea debe ser apoyada a través de un cajero automático, o un dispositivo de vigilancia segura.
- El procedimiento que se debe seguir para cambiar el PIN, sería:
    - Registrarse con el PIN actual
    - Verificar el PIN antes de la selección de cambio de PIN.
    - Activación del nuevo PIN.
    - El nuevo PIN debe introducirse dos veces y el terminal debe confirmar que las dos entradas sean idénticas.
- La aplicación Cambio de Pin debe tener una interfaz de usuario fácil e intuitiva para el titular de la tarjeta, mostrando así claramente instrucciones inequívocas.
- El terminal debe estar diseñado para garantizar que ninguna aplicación cargada de forma no autorizada en la gestión de PIN de datos, pueda ingresar.
- El terminal debe proporcionar una clave de corrección de errores en un solo dígito durante el ingreso de PIN de entrada.

- El terminal debe estar equipado con una pantalla de privacidad.
- Este proceso de cambio de clave se lo puede realizar también vía on-line seleccionando la opción de cambiar PIN por correo.

3.3.3.11 Activación del PIN

- Este proceso de activación del PIN, se lo puede realizar de dos maneras:
    - Activación explícita:
        - El titular de la tarjeta pide el PIN mediante un recibo donde consta el número, el mismo debe estar firmado y verificado.
    - Activación implícita:
        - El tarjetahabiente pide únicamente que le activen el PIN, pero éste no recibe ningún medio físico que contenga el éste número.

3.3.3.12 Desactivación del PIN

- El PIN debe ser desactivado por el emisor, cuando el titular lo requiera, o simplemente cuando ocurra lo siguiente:
    - Se sospecha que el PIN se encuentra comprometido.
    - Todas las cuentas asociadas al PIN están cerradas.
    - El emisor determina que la desactivación es apropiada.
    - Solicitud de desactivación por el titular de la tarjeta.
- El titular de la tarjeta debe ser informado de las medidas adoptadas.
- El emisor debe adoptar medidas apropiadas para garantizar el PIN desactivado.

3.3.3.13 Desbloqueo de PIN

- Los tarjetahabientes después de haber solucionado ciertos inconvenientes, pueden optar por desbloquear el PIN de su tarjeta, para ello los emisores de dichas tarjetas deben implementar una seguridad adicional o adoptar medidas antes de ejecutar la función de desbloqueo de PIN.
- El desbloqueo se puede realizar a través de un cajero automático, en cuyo caso la pantalla ATM debe asesorar a los poseedores de la tarjeta y brindarles orientación inequívoca del procedimiento para desbloquear el PIN.
- Los tarjetahabientes deben ser informados si su PIN se ha desbloqueado con éxito.

3.3.3.14 Gestión de PIN por Internet

- El emisor debe proporcionar al titular de la tarjeta una guía de seguridad para la gestión de PIN, en la cual deben incluirse recomendaciones sobre los riesgos de malware y de almacenamiento de datos de la cuenta en la PC.
- El asesor que brindará ayuda sobre el PIN por Internet debe asegurar que éste se encuentra protegido con algoritmos criptográficos durante toda la transacción, es decir desde que se transmite hasta que llega a la computadora del titular y viceversa.
- Los procesos realizados durante la Gestión de PIN por Internet, se basan en el principio de que jamás se puede asociar el número de control asignada a cada tarjetahabiente con alguna cuenta específica.

- Los valores del número de control y autenticación no deben revelar el número de cuenta del usuario, y los mismos serán comunicados al titular de la tarjeta utilizando un mecanismo diferente.

3.3.3.15 PIN olvidado

- La mente de un ser humano es frágil y a cualquier persona puede olvidarse su PIN, para ello debe tener en cuenta:
    - El nuevo PIN no debe ser sustituido dentro de una transacción.
    - La sustitución del PIN se debe realizar a través de los sistemas del emisor.

3.3.3.16 Procedimientos especiales para la Administración del PIN

- Cuando se utilizan procedimientos para administrar los PIN de usuarios con capacidades especiales, se tiene tratamientos diferentes, por ejemplo, los tarjetahabientes ciegos o con deficiencias visuales, deben ser cuidadosamente controlados y se deben aplicar lineamientos rigurosos para evitar una mayor posibilidad de fraude.

3.3.3.17 Amenazas contra el PIN

- Los emisores de las tarjetas, es decir los que administran los PIN de los usuarios, deben especificar los eventos sospechosos que hacen que un PIN se encuentre comprometido, siendo éste el caso, se debe tomar en cuenta las siguientes recomendaciones:
    - El PIN con amenazas debe desactivarse tan pronto como sea posible.
    - En caso de que el PIN sea desactivado, el titular de la tarjeta debe ser informado de las opciones disponibles para solicitar un nuevo.

- El nuevo PIN no debe ser nada parecido a la clave antes amenazada.
- La activación del PIN de reemplazo puede ser de manera implícita o explícita.
- Las transacciones fraudulentas deben ser reportadas a las redes encargadas de la administración, quienes tomarán acciones.

3.4 Encriptación

Existe información delicada y confidencial como contraseñas, números de tarjetas de crédito, etc., que deben contar con la mayor seguridad, de manera que sea ilegible a terceros, esto se logra gracias a un proceso denominado encriptación, el mismo que se realiza mediante fórmulas matemáticas complejas, ésta información podrá ser manipulada únicamente por aquellas personas que apliquen la clave correcta; la encriptación se trata también de una medida de seguridad que se usa para almacenar o transferir información, éste proceso se lo escribe en un texto plano al que se lo denomina criptograma.

Encriptación, es una mala traducción de la palabra en inglés “encrypt”, por lo que es recomendable utilizar el término "cifrado". (Encriptación. 2013. Encriptación. 10 Diciembre 2013. http://www.alegsa.com.ar/Dic/encriptacion.php).

3.4.1 Criptografía

Desde siempre ha sido importante la comunicación entre las personas, y por lo mismo existe la necesidad de tener mensajes privados a los que solo tengan acceso los destinatarios y que sean entendidos solamente por ellos. Por esta razón se crearon los sistemas de cifrado.

Criptología proviene de las palabras griegas “Kryto” y “logos” que significa estudio de lo oculto; y tiene una rama denominada criptografía, que es la que se ocupa del cifrado de mensajes, además esta se basa en que el emisor manda un mensaje en claro que es tratado mediante un cifrador con la ayuda de una clave, de esta manera se crea un texto cifrado; el mismo que por medio de un canal de comunicación establecido llega al descifrador que convierte el texto cifrado, apoyándose en otra clave, en texto en claro original. Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales dependiendo del sistema que se utilice.

La criptología es una disciplina muy antigua, sus orígenes se remontan al nacimiento de nuestra civilización. Al inicio su único objetivo era el proteger la confidencialidad de informaciones militares y políticas, sin embargo; en la actualidad es una ciencia interesante no solo en esos campos, sino para cualquier otro ámbito que esté interesado en la confidencialidad de datos determinados; ésta se usa tradicionalmente para ocultar mensajes de ciertos usuarios, siendo muy útil ya que las comunicaciones a través de Internet circulan por infraestructuras con una fiabilidad y confidencialidad no garantizada.

Aunque el objetivo original de la criptografía era mantener en secreto un mensaje, hoy en día no se persigue únicamente la privacidad o confidencialidad de los datos, sino que se busca además garantizar la autentificación de los mismos (el emisor del mensaje es quien dice ser, y no otro), su integridad (el mensaje que leemos es el mismo que nos enviaron) y su no repudio (el emisor no puede negar el haber enviado el mensaje).

Algunas civilizaciones antiguas ya utilizaban métodos similares a éste, como por ejemplo, cuando los sacerdotes egipcios utilizaban la escritura hierática o jeroglífica que era incomprensible para el resto de la población; así como también se puede mencionar el uso de la escitala espartana usada durante la guerra entre Atenas y Esparta, la misma que era un palo o bastón en el cual se enrollaba una tira de cuero, sobre la que se escribía el mensaje en columnas paralelas al eje del palo; la tira desenrollada mostraba un texto sin relación con el texto inicial, pero que podía leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero; con este sistema los gobernantes de Espartana transmitieron sus instrucciones secretas a los generales de su ejército durante las campañas militares. Para que se pueda concretar el procedimiento, el emisor y receptor debían contar con un palo o bastón del mismo grosor y longitud. Uno de los métodos de cifrado antiguo más sobresaliente y simple, es el "Cifrario de Cesar", empleado por Julio César en los tiempos de la Roma Imperial, para enviar mensajes secretos a sus legiones, su funcionamiento consiste en sustituir las letras de un documento por la tercera letra que le correspondiese en el alfabeto, es decir, la A se convertía en una D, la B en E, la C en F…. la Z en C.

Con el pasar del tiempo los sistemas criptográficos fueron avanzando en complejidad y funcionalidad, ya que la necesidad de que la información se mantenga segura aumentaba, además la tecnología avanza constantemente, lo que obliga a que todo vaya conforme con el pasar del tiempo.

Tanto el cifrado como el descifrado requieren una clave para realizar sus procedimientos correctamente, las mismas que se dividen en dos tipos:

1. Las claves simétricas: Se usan para el cifrado y para el descifrado con clave secreta.
2. Las claves asimétricas: Se usan para el cifrado y descifrado con clave pública, la misma que debe der distinta en ambos casos.

El término decryption también se refiere al acto de intentar descifrar en forma ilegítima el mensaje ya sea que conozca o no el atacante la clave de descifrado, de manera que si él mismo no conoce la clave de descifrado, se habla de criptoanálisis (decodificación), éste es otra rama de la criptología.

El criptoanálisis es la reconstrucción de un mensaje cifrado en texto simple utilizando métodos matemáticos. Por lo tanto, todos los criptosistemas deben ser resistentes a los métodos de criptoanálisis, cuando un método de criptoanálisis permite descifrar un mensaje cifrado mediante el uso de un criptosistema, decimos que el algoritmo de cifrado ha sido decodificado; se pueden mencionar cuatro métodos de criptoanálisis:

1. Ataque de sólo texto cifrado, el cual consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados.
2. Ataque de texto simple conocido, este consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados conociendo el texto correspondiente.
3. Ataque de texto simple elegido, éste método consiste en hallar la clave de descifrado utilizando uno o más textos cifrados, pudiendo de esta manera el atacante generarlos a partir de textos simples.

4. Ataque de texto cifrado elegido, consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados; el atacante tiene la opción de generarlos a partir de los textos simples.

En el medio de la criptografía se reconocen dos tipos de personas, los criptógrafos y cripto-analistas. Los primeros se ocupan de desarrollar algoritmos de criptografía mientras los cripto-analistas se ocupan de romper los métodos de cifrado para obtener información de manera no autorizada, ambas actividades van de la mano y favorecen al desarrollo de la criptografía.

3.4.1.1 Algoritmos

La encriptación se basa en tres tipos de algoritmos:

- Criptografía clásica
- Algoritmos simétricos (cifrado por bloques)
- Algoritmos asimétricos de cifrado

Los mismos que se explican a continuación.

3.4.1.1.1 Criptografía clásica

Son sistemas que utilizan algoritmos sencillos, simétricos y de fácil análisis para los ordenadores; tienen claves largas con el objetivo de aumentar su seguridad; la Universidad de España, en su publicación describe a la criptografía clásica como:

"*Los métodos clásicos son aquellos en los que, además de las máquinas dedicadas para cifrar, se usan por separado técnicas de sustitución y transposición aplicadas a los caracteres del mensaje en claro. Las técnicas criptográficas utilizadas en este caso son en su totalidad orientadas a sistemas de clave secreta, generalmente manteniendo también en secreto el algoritmo, incluso en el caso en*

que el cifrador cuente con una clave secreta. El cifrado se realiza sobre caracteres alfanuméricos, por lo general alfabéticos, y en ese mismo formato se transmiten o almacenan."(Escuela Universitaria de Informática de la Universidad Politécnica de Madrid-España, 1999).

3.4.1.1.1.1 Métodos de la Criptografía Clásica:

- Transposición inversa. Para ejecutar el algoritmo es necesario conocer el inicio y fin del mensaje, al que se lo invierte mediante éste método, de la siguiente manera:

  Mensaje que se envía: "hola mundo"

  Criptograma: "odnumaloh".

  Es necesario conocer que se usa el mismo algoritmo tanto en cifrado como en descifrado.

- Transposición simple. Éste método separa los caracteres uno por uno, agrupándolos en dos bloques; el primero contendrá los símbolos impares, mientras que el segundo reunirá los caracteres pares; y al final se unirán ambos bloques obteniendo el criptograma, que quedaría de la siguiente manera:

  Mensaje que se envía: "hola mundo"

  Bloque1: hlmno

  Bloque2: oaud

  Criptograma: hlmnooaud

Para descifrar el mensaje se utiliza un proceso similar al de cifrado, con la única diferencia de que al momento de unir los bloques separados anteriormente, se deben intercalar uno a uno los caracteres de cada agrupación.

- Transposición doble. Para poder ejecutar éste procedimiento se debe realizar una transposición simple al mensaje, una vez obtenido el criptograma, sufre otro cambio, pues se efectuara por segunda vez el método de transposición simple; logrando de esta forma conseguir el criptograma final.

  Mensaje que se envía: "hola mundo"

  Primera Transposición Simple:

  Bloque1: hlmno

  Bloque2: oaud

  Criptograma: hlmnooaud

  Segunda Transposición Simple:

  Bloque1: hmoad

  Bloque2: lnou

  Criptograma: hmoadlnou

  Este es un algoritmo sencillo pero de mucha ayuda, pues sirve para despistar a un cripto-analista que intente descifrar mediante transposición simple el criptograma.

- Transposición por grupos. En éste método se utilizan permutaciones, las mismas que harán que el mensaje original anteriormente dividido en bloques de n caracteres se reordene.

Los bloques de elementos del mensaje original, se transmitirán de acuerdo a la clave generada, de la siguiente manera:

Ejemplo:

Clave: 43521.

Mensaje que se envía: Tesis realizada por Gabriela y Belén

División en bloques: TESIS REALI ZADAP ORGAB RIELA YBELE NXXXX

Criptograma: ISSET LAIER ADPAZ AGBRO LEAIR LEEBY XXXXN

Para el método de descifrado se reordenará la clave en el orden original, y se realizará el mismo proceso de cifrado. En este caso la clave sería 54213.

- Transposición por series. Para realizar éste método de cifrado, es necesario ordenar el mensaje original con funciones específicas, las mismas que deberán seguir una secuencia, y al momento de unirlas se formará el criptograma.

Mensaje que se envía: hola mundo

Funciones:

f(1) = números primos = 1,2,3,5 = holm

f(2) = números pares = 4,6,8 = aud

f(3) = números impares = 9 = o

Criptograma: holmaudo

Es importante conocer las funciones que se utilizaron y el orden en las que fueron cifrando el mensaje original, de esta manera se tendrá el número de orden correspondiente a cada elemento y se podrá reordenar el mensaje sin ningún problema.

- Máscara rotativa. Para realizar este método es necesario crear dos matrices de nxn, denominadas, matriz A y matriz B. Cada A[fila,columna] tendrá un elemento que se encuentre o no dentro del mensaje, mientras que en la matriz B, se elegirá algunos elementos pertenecientes a la matriz A y al mensaje original; una vez sobrepuesta la matriz B sobre la matriz A quedarán seleccionados elementos, en cualquiera de sus cuatro lados, siendo la referencia de inicio uno de sus lados.

Ejemplo de cómo gira la matriz B:

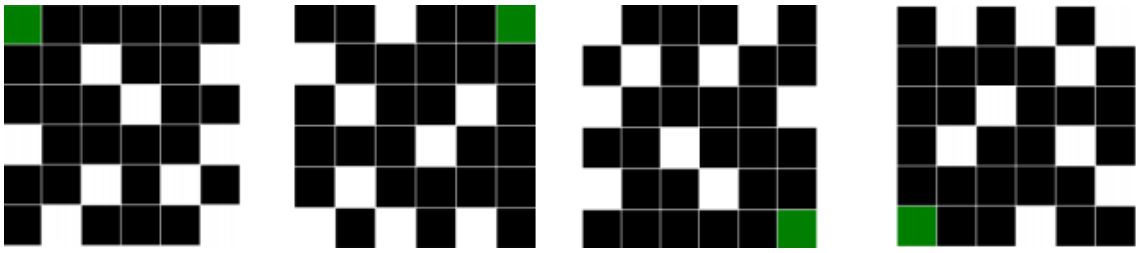


Figura 18. Máscara Rotativa. http://genomorro.files.wordpress.com/2007/09/trabajo.pdf

Los espacios en blanco que se observan en el grafico son los que corresponden a los elementos del mensaje y cada posición de la matriz se lee de arriba hacia abajo; y de derecha a izquierda.

- Sustitución por desplazamiento. Es un método que utiliza un algoritmo parecido al "Algoritmo de César", es decir se toma una letra como clave, y cada caracter del mensaje original se desplazará tantos espacios como indique la clave y ahí obtendrá un nuevo valor, el mismo que corresponderá a otra letra, cabe recalcar que la clave usada puede ser un solo elemento o una frase. Para realizar el ejemplo, se tomará como referencia el alfabeto, donde la letra A corresponde al número 1 y la Z al 26, sin tomar en cuenta la letra Ñ.

Mensaje que se envía:	H	O	L	A
Posición de las letras del mensaje actual:	8	15	12	1
Clave	C	C	C	C
Clave	3	3	3	3
Criptograma:	11	18	15	4
Criptograma:	**K**	**R**	**Q**	**D**

Tabla 1. Ejemplo de Sustitución por desplazamiento

En el caso de que la suma de la posición actual de la letra del mensaje en claro más la clave, sea mayor a la equivalencia de la posición del último elemento, se deberá restar a éste el valor de la clave.

Para descifrar el mensaje se debe realizar la operación contraria, es decir la resta, utilizando el mismo mecanismo.

- Algoritmo de Vigenere. Para poder realizar el cifrado bajo éste método se debe utilizar la Tabla de Vigenere, misma que es una matriz cuadrada de caracteres:

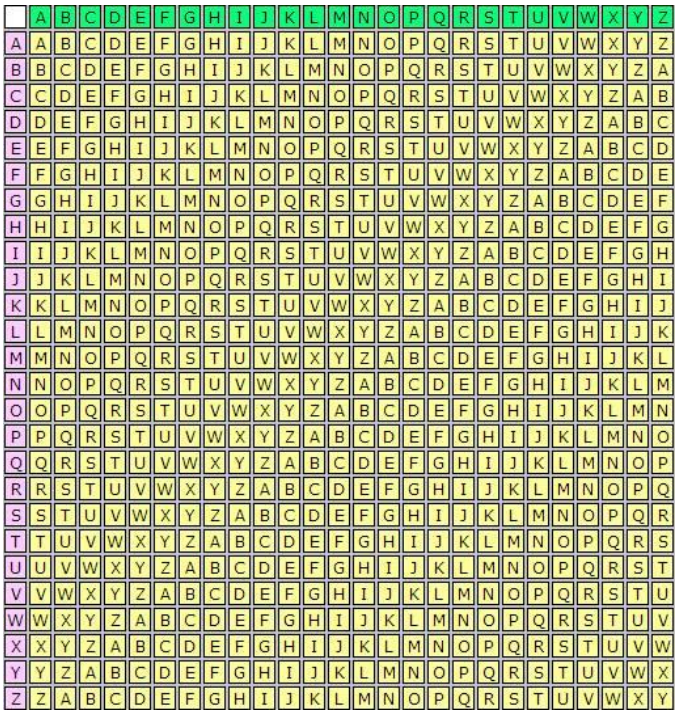


Figura 19. Algoritmo Vigenere, http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRIPTOGRAFIA/POLIALFABETICAS/cifra%20de%20vigenere.html

La fila del encabezado de esta matriz representa cada uno de los caracteres del mensaje que se va a enviar, mientras que la columna principal indica la clave mediante la cual se cifrará el mensaje; al seleccionar la intersección de éstos dos elementos, nos da el carácter ya cifrado, por ejemplo la letra B cifrada con la clave G nos dará el criptograma H.

En términos matemáticos puede expresarse como:

Yi = (Xi + Zi)modT , donde:

Xi = posición de la letra del mensaje por enviar

Zi = clave asignada

T = número de letras del alfabeto

Con Zi = G,A,B,E

Mensaje que se envía:	GABY	BELEN	TESIS	EXITOSA
Clave	GABE	GABEG	ABEGA	BEGABEG
Criptograma:	**MACC**	**HEMIT**	**TFWOS**	**FBOTPWG**

Tabla 2. Ejemplo Algoritmo Vigenere

Es necesario conocer que a una misma letra del mensaje a enviar le pueden corresponder diferentes letras en el texto cifrado.

Para descifrar el mensaje se debe colocar cada letra del criptograma en la parte central de la matriz, y fijarse en la fila que corresponda según su clave, entonces con esa intersección, se conocerá con claridad a que columna pertenece, y esa será el carácter del mensaje que le corresponda.

3.4.1.1.2 Criptografía Simétrica

Este tipo de criptografía utiliza una única clave para realizar el cifrado y descifrado de mensajes, la misma que deberá ser conocida previamente por el emisor y receptor del mensaje; sabiendo que la forma de transmitir la clave es insegura, pues se lo haría por correo electrónico, mensaje de texto, en voz alta o por medio de llamadas telefónicas, lo que resulta de fácil interceptación.

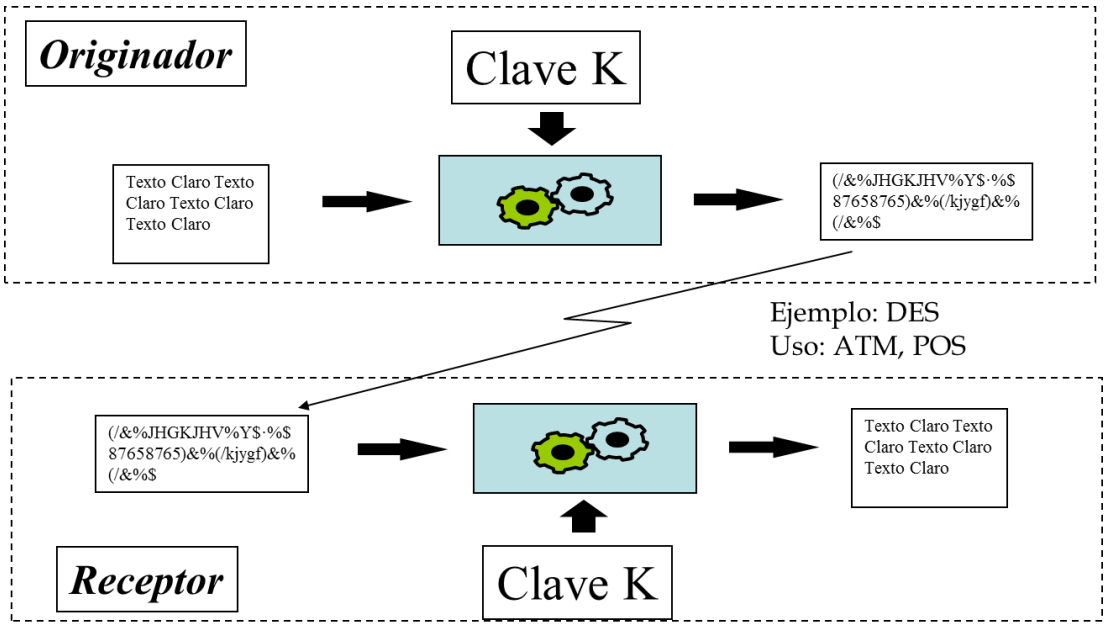


Figura 20. Criptografía Simétrica. (Ing. Pablo Pintado, 2012)

Hay que tener claro que la seguridad de un mensaje cifrado jamás recaerá sobre un algoritmo, pues sería tarea fácil para los hackers, manipular la información; por el contrario, la misma debe recaer siempre sobre la clave.

Uno de los dispositivos que manejaban métodos simétricos para cifrar el mensaje es la máquina Enigma, la misma que generaba un abecedario diferente dependiendo de la posición en la que se encuentren los rodillos, ésta máquina contenía una especie de libro con diversas claves, entre las cuales se encontraba la "clave del día", de ésta manera aseguraban la información, pues jamás tendría la misma clave dos días seguidos.

3.4.1.1.2.1 Tipos de Criptografía Simétrica

- Cifrado Producto.
- DES.
- IDEA (International Data Encryption Algorithm).

- Algoritmo de Rijndael (AES).
- Modos de Operación para Algoritmos de Cifrado por Bloques.

3.4.1.1.3 CIFRADO PRODUCTO.

Es una técnica que consiste en dividir el mensaje y colocarlo en bloques de tamaño fijo, y a cada uno de éstos se le debe aplicar una función de cifrado; cabe recalcar que sería suficiente realizar lo que en la Criptografía Simétrica se la conoce como "Confusión", la misma que realiza sustituciones complejas entre el texto normal, el cifrado y la clave; tratando de ésta manera ocultar la relación que existe entre ellos; la desventaja de utilizar dicho método es que ocuparía demasiada memoria. Otro concepto fundamental en éste cifrado es la "Difusión", la misma que realiza permutaciones, tratando de ésta manera, repartir la influencia de cada bit del mensaje que se va a enviar en el mensaje cifrado.

3.4.1.1.4 ALGORITMO DES

Es el algoritmo simétrico más usado mundialmente, es muy rápido y fácil de implementar, pero su problema es que usa una clave de descifrado muy corta, lo que facilita los robos y fraudes en la información. Según una investigación realizada en la Universidad Pontificia "Comillas" de Madrid, el algoritmo DES, trabaja de la siguiente manera:

"*Codifica bloques de 64 bits empleando claves de 56 bits. Es una Red de Feistel de 16 rondas, más dos permutaciones, una que se aplica al principio (Pi) y otra que se aplica al final (Pf), tales que* $Pi = P - 1\ f$ *. La función f se compone de una permutación de expansión (E), que convierte el bloque de 32 bits correspondiente en uno de 48.La realizan las denominadas cajas E y son fijas para*

todas las implementaciones del DES. Después realiza un or-exclusivo con el valor Ki, también de 48 bits, más tarde pasan a las S-Cajas que son las más importantes del DES, reciben 48bits y sacan solamente 32 mediante una compresión. Tiene en total 8 cajas, a cada una de ellas le entran 6 bits y salen 4." (Universidad Pontificia Comillas ICAI, Madrid 2006).

Para realizar el descifrado de éste algoritmo se utiliza el mismo método solo que usando un orden inverso.

Para garantizar la seguridad de la información, el método DES ha sufrido algunas variantes, como por ejemplo:

- DES Múltiple. Donde se emplea varias veces el algoritmo DES, cada una de ellas con una clave diferente.
- Triple-DES. Para la cual se sigue un proceso de obtención de clave, es decir primero se codifica con una subclave denominada k1, luego se decodifica con k2 y en seguida se vuelve a codificar con k1, como resultado se tiene la unión de k1 y k2, la misma que sería la clave final y su tamaño de 112 bits.

3.4.1.1.5 IDEA (International Data Encryption Algorithm)

Es un algoritmo seguro, de uso libre, con poca probabilidad de ataques ya que tiene una clave muy extensa, éste fue desarrollado y liberado en 1991 por Xuejia Lai y James L. Massey del Politécnico de Zurich, el mismo que codifica bloques de 64 bits empleando una clave de 128 bits, generando así 52 subclaves para encriptar y otras 52 para descencriptar, cada una de ellas de 16 bits.

El algoritmo de encriptación IDEA realiza operaciones en cada una de sus iteraciones (8 en total), las mismas que consisten en dividir a un bloque de 64 bits en 4 partes iguales de 16 bits cada una; para cada una de las iteraciones se utilizan 6 subclaves y para la transformación final las 4 subclaves restantes. El algoritmo que se usa para descifrar los mensajes es el mismo que el empleado al momento de cifrar los mismos.

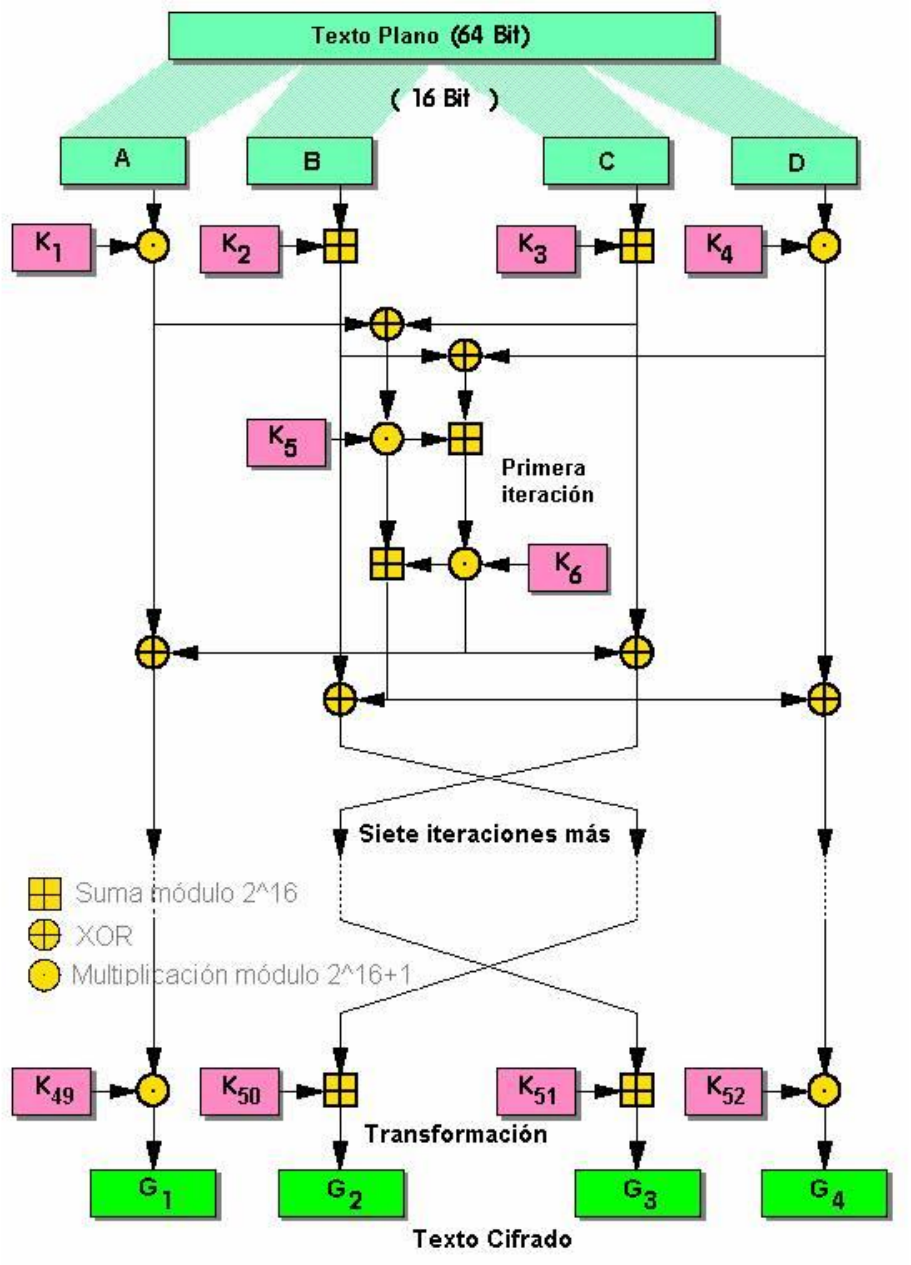


Figura 21. Idea (http://iie.fing.edu.uy/ense/asign/dsp/proyectos/1999/cripto/descripcion.html)

3.4.1.1.6 ALGORITMO DE RIJNDAEL (AES)

Al algoritmo de DES se lo sustituyó por RIJNDAEL, el cual fue adoptado por el NIST (National Institute for Standards and Technology) en el 2000, oficialmente, como nuevo Estándar Avanzado de Cifrado (AES), ya que el mismo contempla múltiples virtudes como la confiabilidad, seguridad, resistencia al criptoanálisis lineal y diferencial, se le puede otorgar varias aplicaciones criptográficas, e impide la detección de manera fácil a los hackers; es necesario conocer que el proceso de selección, revisión y estudio de éste algoritmo fue realizado de forma pública, es decir su análisis fue desarrollado por toda la comunidad criptográfica mundial. El nombre RIJNDAEL tuvo origen con la unión de los apellidos de sus dos creadores J. Daemen y V. Rijmen. RIJNDAEL es un sistema de cifrado por bloques que maneja longitudes de clave y de bloque variables, comprendidas entre los 128 y los 256 bits; está formado por varias iteraciones, las cuales dependen del tamaño de bloque y clave elegidos; cada una de éstas reiteraciones aplica 4 funciones (ByteSub, ShiftRow, MixColumn, AddRoundKey), las mismas que darán como resultado el bloque cifrado requerido.

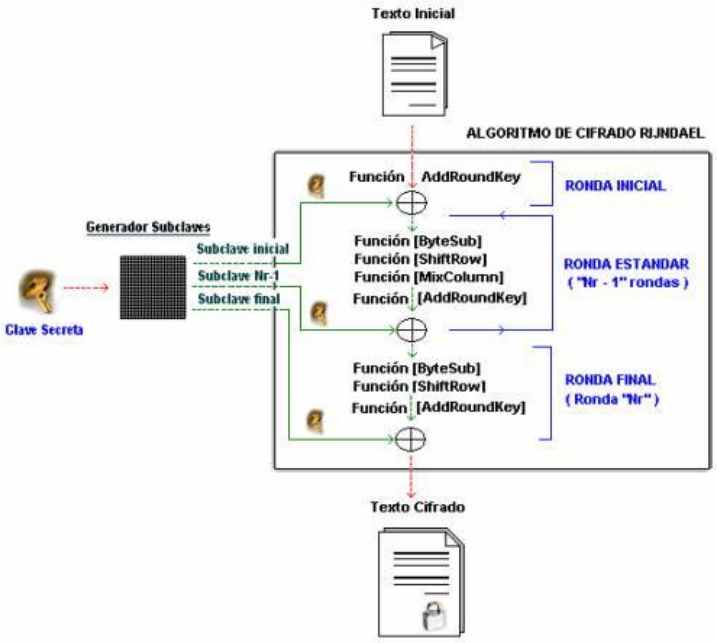


Figura 22. Algoritmo de Rijndael (http://www.tierradelazaro.com/cripto/AES.pdf)

El algoritmo de descifrado consiste en aplicar a cada una de las funciones su inverso y en orden contrario, de ésta manera se obtendrá el mensaje enviado.

3.4.1.1.7 Modos de operación para algoritmos de cifrado por bloques

Existen mecanismos independientemente del método de cifrado que se utilizan para añadir información al final del mensaje, cuando el mismo no tiene una longitud que sea múltiplo exacto del tamaño de bloque, éstos pueden ser:

- Rellenar con ceros el bloque que se codifica hasta que se complete el mismo, pero en éste mecanismo se encontrará un gran problema, pues al momento de descifrar se debe conocer exactamente por donde se cortará el bloque, para ellos será necesario que se agregue como último byte del último bloque el número de bytes que se han aumentado.

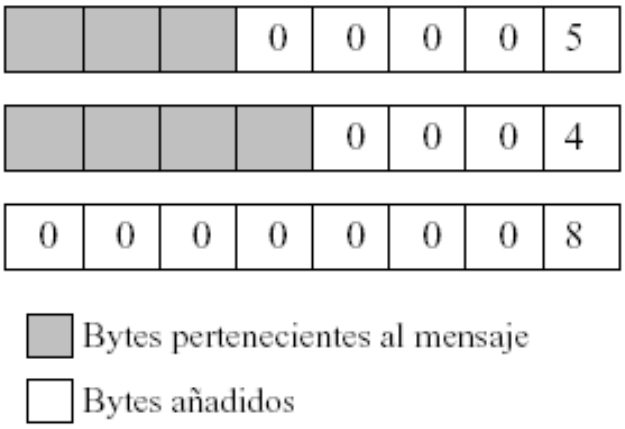


Figura 23. Bloque con ceros. (http://www.docstoc.com/docs/104692743/Algoritmos-criptogr%25EF%25BF%25BDficos)

Los algoritmos simétricos encriptan bloques de texto de longitud fija, es decir, el tamaño del texto cifrado luego de haber sufrido transformaciones, será el mismo que el tamaño del texto original, como los tamaños de los bloques pueden ser variables, y si se tiene un mensaje muy extenso, se usan los modos de operación, los mismos que son:

- ECB

- CBC
- CFB
- OFB

3.4.1.1.7.1 Modo ECB (Electronic Code Book)

Es un método sencillo que divide el texto en bloques de tamaño fijo, y permite que cada uno de ellos sea cifrado por separado pero utilizando la misma clave.

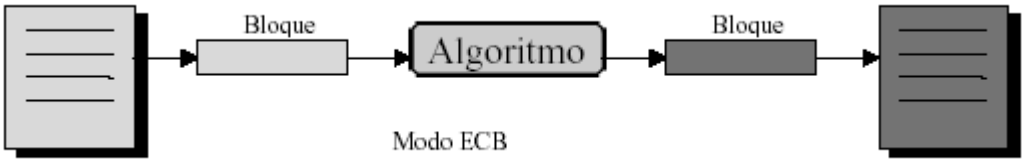


Figura 24. Modo ECB (Ing. Belén García Lobo)

Ventajas	Desventajas
Permite encriptar y descencriptar bloques independientemente de su orden.	Si se envían textos iguales, se obtendrá bloques de texto cifrado iguales.
Fácil implementación	Los criptoanalistas podrían reconstruir el texto, sin conocer la clave empleada.
Poca probabilidad a errores.	Sustitución de bloques similares.

Tabla 3. Ventajas y Desventajas ECB

3.4.1.1.7.2 Modo CBC (Cipher Book Chaining)

Este modo consiste en ir encriptando encadenadamente los bloques de texto, de manera que cada uno de ellos dependa exclusivamente de su antecesor, es decir se

aplica una operación XOR entre el texto original del bloque a encriptar y el texto cifrado del bloque anterior, finalmente el último bloque se encriptará con la clave.

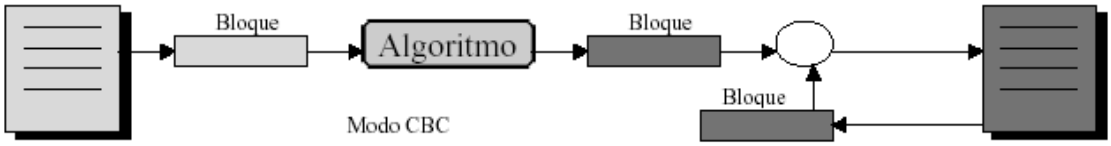


Figura 25. Modo CBC (Ing. Belén García Lobo)

Ventajas	Desventajas
No se da la sustitución de bloques.	Dos bloques de texto pueden ser iguales, por lo que se obtendrá el mismo resultado (Vector de Inicio)
Modo Robusto.	Propagación de errores.

Tabla 4. Ventajas y Desventajas CBC

3.4.1.1.7.3 Modo CFB (Cipher Feedback Mode)

Se debe encriptar el mensaje en elementos más pequeños que el tamaño del bloque, sabiendo que la continuidad de éstos nos dará la secuencia de la clave; éste proceso se llevará a cabo con la ayuda del Algoritmo DES. Para que se modifique la secuencia de la clave, se realiza la función XOR entre los caracteres encriptados y el Vector de inicialización.

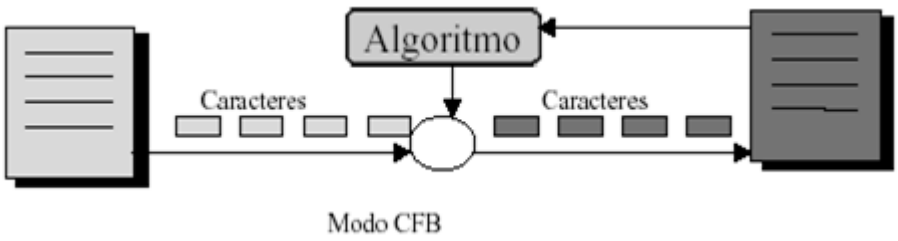


Figura 26. Modo CFB (Ing. Belén García Lobo)

Ventajas	Desventajas
Mayor seguridad en el canal de transmisión para las comunicaciones.	Propagación de errores.
Se utiliza para generar códigos de autenticación MAC.	
Aprovechamiento de la capacidad de transmisión en su totalidad.	

Tabla 5. Ventajas y Desventajas CFB

3.4.1.1.7.4 Modo OFB (Output FeedBack Mode)

Su proceso es similar al que utiliza el Modo CFB, con la única diferencia de que la secuencia de la clave no es dependiente de la continuidad de los datos.

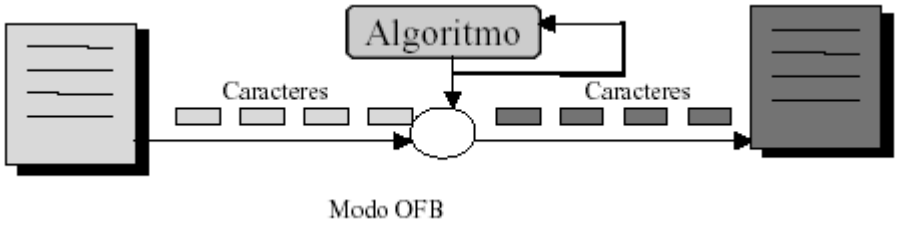


Figura 27. Modo OFB (Ing. Belén García Lobo)

Para poder des encriptar el mensaje se debe realizar una sincronización entre claves del receptor y emisor.

Ventajas
No existe propagación de errores.
Se utiliza para la generación de números pseudoaleatorios.

Tabla 6. Ventajas OFB

3.4.1.1.8 Criptografía Asimétrica

La criptografía asimétrica utiliza dos claves para poder enviar un mensaje: la pública (que se encuentra al alcance de cualquier persona) y la privada (que debe conocer solo el propietario). Esta criptografía tiene varias ventajas, entre ellas está la que ya no es necesario que el emisor y receptor del mensaje acuerden en la clave a utilizar, al contrario el receptor del mensaje podrá abrirlo siempre y cuando conozca la clave pública

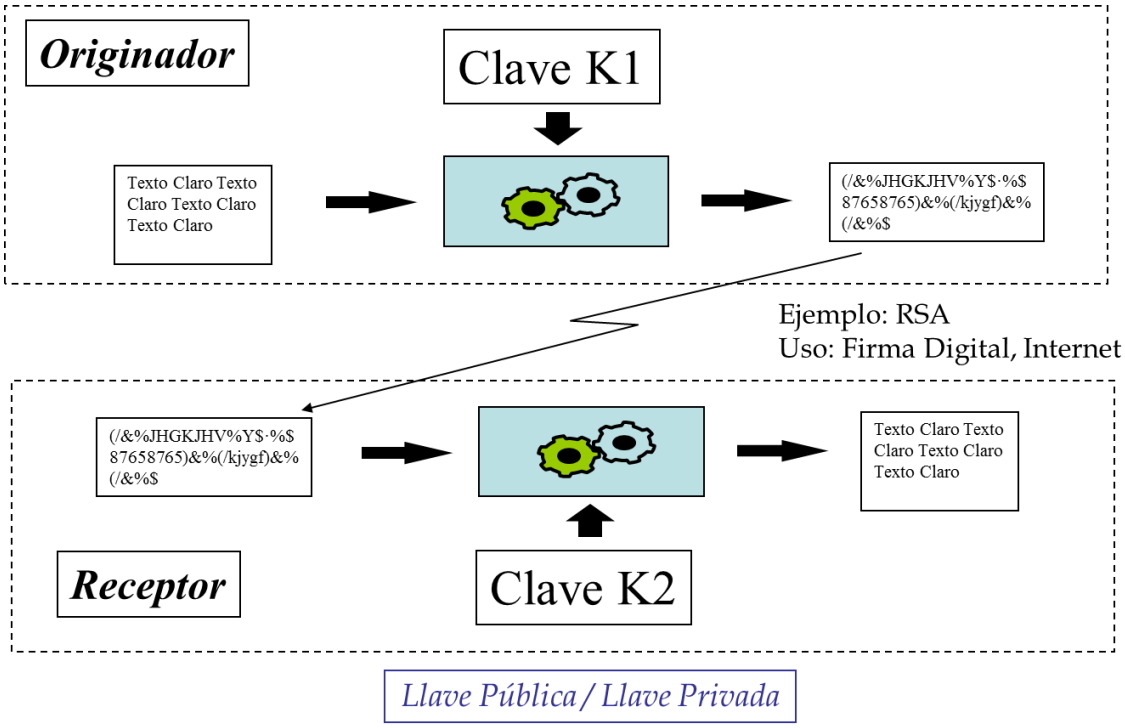


Figura 28. Criptografía Simétrica (Ing. Pablo Pintado, 2012)

A partir del desarrollo de la Criptografía Asimétrica, nace la idea de realizar firmas digitales, ya que seguirían el mismo proceso, pues se logrará identificar y autentificar a la persona que envía el mensaje original por su clave privada, mientras que los receptores que conozcan la clave pública solo se limitarán a leer el contenido. De ésta manera se afirma el propósito de los Criptogramas asimétricos, que es el de poder firmar documentos, afirmando que el remitente es quien dice ser.

Es por ello, que se dice que los métodos asimétricos se emplean para intercambiar la clave de sesión mientras que los simétricos para el intercambio de información dentro de una sesión.

Los algoritmos asimétricos se listan a continuación:

- RSA
- DH - Diffie-Hellman
- El Gammal
- Rabin
- DSA - Digital Standard Algorithm

3.4.1.1.8.1 RSA

Ron Rivest, Adi Shamir y Leonard Adleman, en 1977 crearon el algoritmo denominado RSA, (lleva este nombre en alusión a la primera letra del apellido de cada uno de los autores). En la actualidad gracias a su sencillez, facilidad de comprensión e implementación y seguridad en la información, es el más utilizado, aunque su desventaja es la gran longitud de sus claves que originalmente fueron de 200 bits, pero con el paso del tiempo han llegado a los 2048 bits; el RSA es la fusión de dos algoritmos muy importantes, el Máximo Común Divisor de Euclídes (Grecia 450-377 A.C.) y el del Teorema de Fermat (Francia 1601-1665).

Se utilizan números primos de varios dígitos (100 a 300) elegidos aleatoriamente para generar claves públicas y la privada, las mismas que serán desarrolladas bajo distintas funciones matemáticas, en la actualidad éstas claves deben contener al menos 1024 bits para mantener protegida los datos.

Para cifrar mensajes con el algoritmo RSA se utiliza la función exponencial discreta, la que aparentemente es muy fácil descifrarla, pero se debe conocer que para el descifrado se utiliza la función inversa, es decir se debe encontrar las raíces

de Ø, lo cual resulta imposible, pues para realizarlo hay que conocer la clave privada.

A pesar de que la seguridad es una de las ventajas más significativas en éste algoritmo ya que las claves privadas son bastante grandes y serán muy difíciles de averiguarlas, se tiene un problema pues el gran tamaño de dichas claves, no permiten la rapidez necesaria, es decir La velocidad de procesamiento será cada vez menor, lo que hará a RSA un método lento.

3.4.1.1.8.2 DH - Diffie-Hellman

Para transmitir un mensaje privado, se requiere que éste sea encriptado, y para que el receptor pueda leerlo debe tener la clave, para ello se debe crear un medio seguro en donde generarla, sin que terceros puedan tenerla; para esto se debe ocupar el algoritmo DH, ya que éste permite intercambiar claves a través de un canal seguro.

Para cifrar un mensaje con el algoritmo DH, se requiere que ambas partes, tanto emisor como receptor escogen dos números, un privado y un público, a los que se les aplica varias funciones matemáticas y operaciones de exponenciación; generando de ésta manera las claves privadas, las mismas que pueden ser enviadas al emisor o receptor por medios públicos.

3.4.1.1.8.3 El Gamal

Es un algoritmo criptográfico creado por Taher El Gamal en 1984 y se basa en emplear una clave pública para cifrar o también para crear firmas digitales, es un algoritmo muy seguro pues se usan funciones de logaritmos discretos con números enteros extensos. La mayor ventaja de éste es que si se envía el mismo mensaje varias veces, puede tener un cifrado diferente para cada envío; sin embargo, uno de

los grandes inconvenientes es el espacio, pues el tamaño del mensaje cifrado puede ser el doble del de mensaje original.

Para la encriptación de los mensajes según el algoritmo de El Gamal, se requiere seguir procesos similares a los realizados con el algoritmo DH, es decir basándose fundamentalmente en operaciones matemáticas exponenciales, que no permitan una fácil desencriptación realizando el procedimiento inverso.

3.4.1.1.8.4 Algoritmo de Rabin

Este Algoritmo fue propuesto por Michael O. Rabin en 1979, el mismo que al ser asimétrico debe contar con dos claves, la pública y privada respectivamente, al igual que RSA se eligen dos números primos aleatoriamente pero ambos deben tener el ultimo bit igual a uno, eso quiere decir, que éstos deben ser n1= n2= 3(mod4) y así se genera la clave privada; y el producto de los mismos sería la clave pública.

Una vez creadas las claves se utiliza la siguiente fórmula para el cifrado: $c= m^2 \pmod n$, donde m es el mensaje a enviar y n es la clave pública; es una función bastante sencilla para cifrar pero es muy seguro pues tiene gran complejidad para el descifrado, ya que es necesario conocer los dígitos primos para poder realizar la raíz cuadrada de mod n, caso contrario se obtendrán cuatro posibles soluciones de las cuales solo el emisor sabrá cuál es el real.

3.4.1.1.8.5 Algoritmo DSA (Digital Signature Algorithm)

El Algoritmo de Firma Digital fue propuesto por la NIST en 1991, usado principalmente para las firmas digitales, ya que su objetivo es el de firmar, no el de cifrar información; con ésta es más fácil verificar la autenticidad de un mensaje, pues para éste proceso se requiere de una clave pública y la firma del mensaje. Cabe

recalcar que el proceso para generar la firma es más rápido que el de la verificación. Su funcionamiento se puede describir en 3 etapas: la primera es la generación de claves, la segunda la creación de firma; éstas dos son realizadas por el emisor del mensaje; y la tercera etapa realizada por el receptor es la verificación.

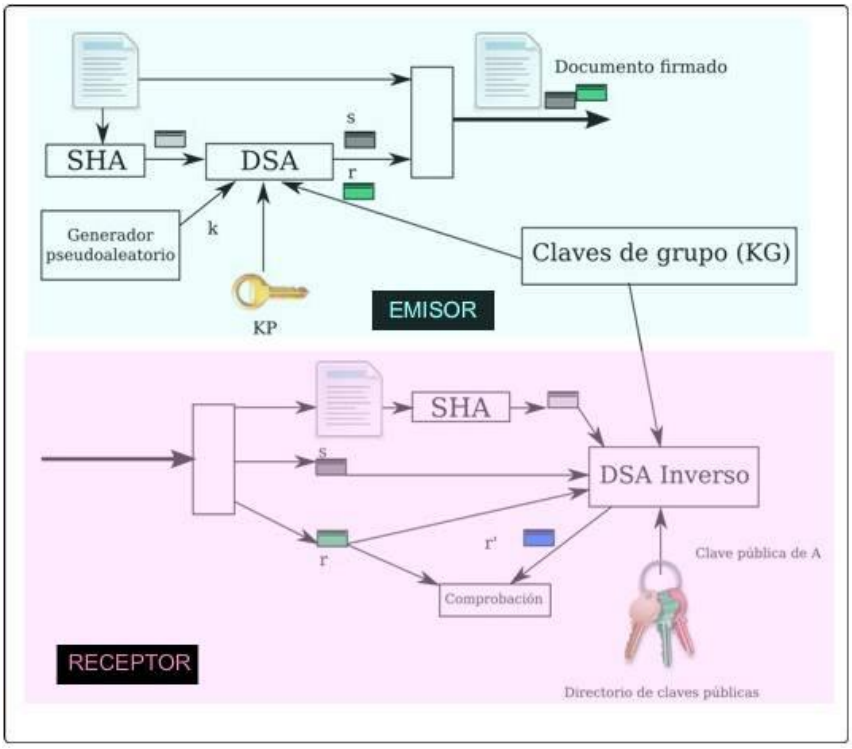


Figura 29 Algoritmo DSA. (http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/5-criptografia-asimetrica-o-de-clave-publica/56-firmas-digitales/562-dsa-digital-signature-algorithm)

Este algoritmo brinda una mayor protección, por lo que utiliza varios parámetros, como:

- KG -> Claves públicas de grupo. Son claves públicas creadas para un conjunto de usuarios.
- KU -> Claves públicas. Es creada para cada usuario dependiendo de la KG que tenga.

- KP -> Claves privadas. Se genera una para cada usuario, dependiendo de la clave pública de los mismos.
- K -> Número aleatorio. Son números generados que se utilizan para cada firma digital.

Este algoritmo es una variante del método asimétrico de ElGamal, pero tiene una desventaja que es la necesidad de más tiempo de cómputo.

3.4.1.2 Aplicaciones

Existen en el mercado varias aplicaciones para la criptografía, el mismo que ofrece una amplia oferta que permite encriptar la información almacenada en dispositivos de todo tipo, las mismas que se podrían clasificar en tres grupos como:

- Aplicaciones que permiten la creación de unidades o volúmenes cifrados. Estas suelen ser las más usadas, ya que encriptan los archivos y carpetas que se almacenan en la unidad o contenedor cifrado.
- Las aplicaciones que cifran carpetas. Estas encriptan una carpeta del disco duro con todo su contenido.
- Aplicaciones que cifran ficheros individuales.

Software libre para cifrar archivos explicados en la clasificación anterior:

- 1 Second Folder Encryption Free: Esta convierte carpetas codificadas en objetos que no podrían ser renombrados, modificados, eliminados o movidos a otra ubicación sin conocer la clave de encriptación.
- Criptod: Esta aplicación requiere la instalación de la Máquina Virtual de Java. Además es necesario que disponga del programa tanto para cifrar como

para descifrar la información. El algoritmo de encriptación que empleará no es conocido, podría dar la impresión de que éste es inmune a los ataques, pero por otro lado, no permitirá evaluar con qué seguridad se protegerá la información cifrada.

- Abi-coder: Permitirá tanto el cifrado de archivos individuales como el de los incluidos en carpetas, también admitirá la creación de ficheros autoextraíbles, que no necesitarán la aplicación para ser descifrados.
- AxCrypt: Lo que más se destaca en esta herramienta es que permitirá la creación de ficheros auto-contenidos, que no requerirán tener instalada la aplicación para ser descifrados; también ofrece una opción para que los datos puedan destruirse de forma definitiva y no puedan restaurarse con herramientas de recuperación avanzada de discos.
- TrueCrypt: Este permite cifrar tanto particiones de disco existentes como guardar ficheros codificados, creando volúmenes virtuales accesibles y ocultos, el tamaño de estos volúmenes virtuales sería totalmente configurable. En cuanto al sistema de cifrado permitirá seleccionar entre distintos algoritmos o combinaciones de ellos.

A continuación una lista de algunos software de aplicaciones de la criptografía:

- GNU Privacy Guard, GnuPG o GPG
- AxCrypt
- John the Ripper
- PGP
- WinCuaimaCrypt
- Cifrado de Discos duros y particiones

- FreeOTFE
- PointSec
- Safeboot
- SafeguardDisk
- TrueCrypt
- Dm-crypt

3.4.1.3 Protocolos

Un protocolo realiza funciones relacionadas con la seguridad, aplicando métodos criptográficos, describiendo la forma en la que un algoritmo debe utilizarse; además, es lo suficientemente detallado en sus estructuras de datos y representaciones, es por ello que para cifrar y proteger la información que se transmite en la Web se utiliza Secure Socket Layer SSL, siendo éste un protocolo que negocia la comunicación segura a nivel de socket, de manera que sea invisible tanto al usuario como a las aplicaciones que lo usan.

El sistema de protocolos se basa en una aplicación conjunta de Criptografía Simétrica, Criptografía Asimétrica (de llave publica), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través del Internet, permitiendo así el intercambio de datos confiables entre dos aplicaciones, principalmente entre un servidor Web y un navegador.

El protocolo SSL se inserta entre la capa TCP/IP de bajo nivel y el protocolo de alto nivel HTTP dentro de la arquitectura de red, además SSL ha sido diseñado principalmente para trabajar con HTTP.

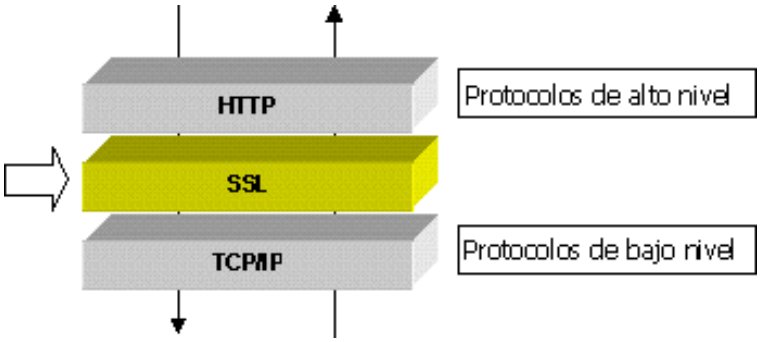


Figura 30 SSL (http://www.4d.com/4d_docstatic/4D/12.4/Utilizar-el-protocolo-SSL.300-977193.es.html)

Como se explicó anteriormente este protocolo establece comunicaciones seguras, es por eso que el usuario para proceder con el pago debe llenar un formulario con sus datos personales, los bienes comprados y al momento del pago la verificación de la información.

Los protocolos poseen ventajas como:

- La autenticación de las partes que intervienen en la compra es decir, el cliente, el comerciante y los bancos.
- La confidencialidad e integridad que con técnicas criptográficas impiden el acceso a la información del pago, así también evitando que el banco acceda a la información de la compra.
- La gestión del pago, el mismo que verifica el registro del titular y del comerciante, autorizaciones y liquidaciones de pagos, entre otras.

En el siguiente gráfico se explica detalladamente la funcionalidad del protocolo SSL:

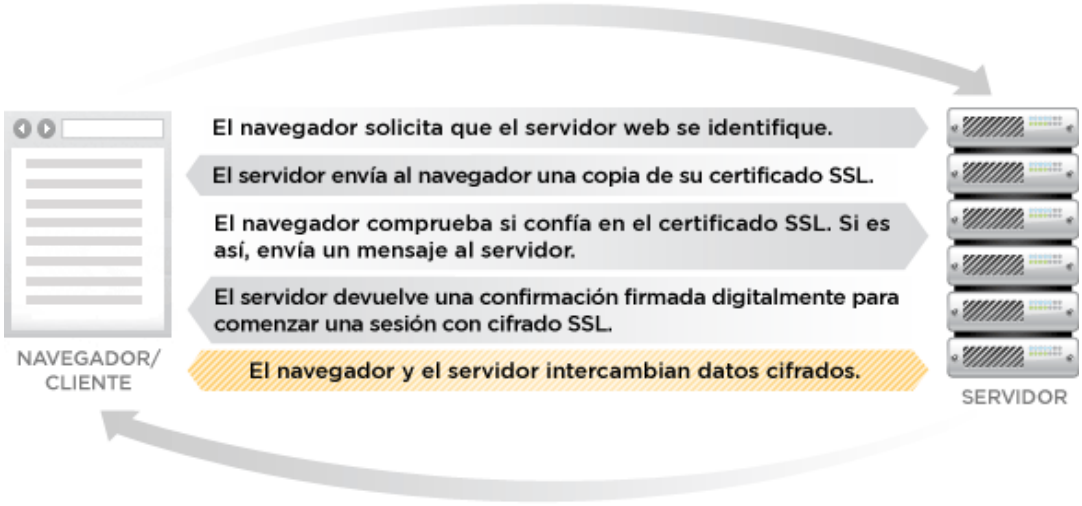


Figura 31. Protocolo SSL. (http://www.expresionbinaria.com/certificados-de-seguridad-ssl-funcionamiento-tipos-y-caracteristicas/)

3.4.1.4 Seguridad

Cada vez aumenta el número de organizaciones que deciden encriptar los datos almacenados en sus sistemas para evitar las consecuencias negativas de posibles pérdidas o robos de información; para aplacar las preocupaciones de los usuarios quienes navegan en la web, se pone a disposición la conformidad con PCI DSS (Payment Card Data Security Standard); siendo éste un estándar de seguridad que ha sido desarrollado para el mejoramiento del control en los datos del usuario con sus tarjetas de crédito en la red; la facilidad de adquirir medidas de seguridad consistentes a nivel mundial fueron desarrolladas en el 2006 por un comité denominado PCI Security Standards Council, en la cual participaron las compañías de tarjetas más importantes como: American Express, Discover Financial Servicces, JCB International, MasterCard WorldWide y Visa Inc.

La función de este estándar es entregar requisitos técnicos para asegurar la información de las personas que poseen tarjetas, de esta manera se prevendría los

fraudes que se dan en el internet. Todos los comerciantes y proveedores que manejan los datos de los titulares exigen el cumplimiento del estándar; la validación de dicha información es realizada por los auditores calificados de QSA (Qualified Seccurity Assesor), quienes están habilitados para estar al tanto del cumplimiento de este estándar.

El estándar PCI tiene como objetivo que los comercios electrónicos posean medidas de control de acceso al mismo, manteniendo el menor grado de vulnerabilidad posible ante los ataques y fraudes producidos en línea, esto será viable si es que diariamente se monitorea y regularmente se comprueba que las redes sean seguras, de ésta manera el usuario podrá tener mayor confiabilidad pues sus datos estarán protegidos gracias a la política de seguridad de la información.

Otro estándar de pago seguro es el PA DSS (Payment Application Data Security Standard), el mismo que tiene como objetivo brindar seguridad a los proveedores de software, evitando el almacenamiento de información que comprometa al tarjetahabiente como los dígitos completos de la banda magnética, el valor del PIN, el CVV2 (valor de verificación de la tarjeta); además de hacer cumplir con las reglas descritas en el protocolo PCI DSS. Este estándar está basado en las buenas prácticas de pago PABP (Payment Application Best Practices), que Visa proporciona a los proveedores de aplicaciones, las mismas que son voluntarias y aseguran que las aplicaciones de pago no almacenan datos engañosos.

Otra norma que recoge los requisitos de seguridad para transacciones con PIN es PCI PTS (PIN Transaction Security), la misma en la que están estipulados las políticas necesarias para el diseño y fabricación de los dispositivos de pago, así como

también la manera en la que se van a transportar dichos dispositivos hacia las empresas que los requieran.

Otro método que brinda protección a la información de los tarjetahabientes es la tarjeta de Módulo de Seguridad Hardware Industria de Pago (PCI_HSM), la primera versión (v1.0) que fue publicada en abril del 2009, siendo éste el primer documento de la Industria de Tarjetas de Pago Security Standards Council (PCI SSC), el mismo que sirve para definir un conjunto de normas lógicas y físicas de seguridad para los sitios donde se manejan los pagos. En mayo del 2012 se publicó una nueva versión (v2.0), y en la actualidad los métodos de pago se basan en el sistema FIPS 140-2, el cuál proporciona confianza y seguridad en los sitios que poseen dispositivos de pagos.

CAPITULO 4. Formas de Pago

4.1 Tipos de formas de pago

Cuando se habla de “pagos”, se hace referencia al dinero que se entrega a una persona, natural o jurídica, a cambio de un bien o servicio recibido, dicho dinero puede ser entregado de varias maneras: personal, virtual o por terceros. Al realizar transacciones, es decir “comercio en línea”, la forma en la que se paga es a través del internet, mediante tarjetas de crédito, y con grades seguridades como Visa y MasterCard, o también con intermediarios como por ejemplo PayPal.

4.1.1 PayPal

Peter Thiel y Max Levchin autores de PayPal creado en 1998 con el nombre “Confinity” con el fin de realizar posibles transferencias monetarias, luego de un año se desarrolla un “demo” en línea permitiendo pagos por correo electrónico. PayPal consigue 1 millón de usuarios en todo el mundo en el año 2000, posteriormente en octubre del 2002 (Historia. 2013. PayPal. 01 Abril 2014. https://www.paypal-media.com/es/history) eBay Inc. compra PayPal e integra la fuerza del mercado en línea con el sistema de pagos número uno en la red, tras pasar dos años en el 2004 se desarrollan las primeras APIs para futuras aplicaciones y servicios de pago en línea. En mayo del 2005 PayPal opera como primera vez en España dando como opción a los usuarios manejar el dinero a través de mensajes de texto mediante móviles a cualquier hora en cualquier lugar; generando el pago exprés; es por ello que PayPal se abre hacia Europa gracias al sector financiero de Luxemburgo que le concedió una licencia bancaria en marzo del 2007. (Historia. 2013. PayPal. 01 Abril 2014. https://www.paypal-media.com/es/history).

En Octubre del 2008, PayPal dio paso a un crédito transaccional a sus clientes al momento de la compra, por la gran aceptación de la sociedad hacia el servicio en el año 2009 PayPal logró el primer millón de cuentas activas; por lo que se decidió lanzar el servicio para envío y recibo de dinero desde un móvil; además una plataforma de pagos global llamada "PayPal X". En el 2010 genera una alta expectativa pues se lanza una aplicación para iPhone, al mismo tiempo se crea una nueva solución para el pago de productos digitales; la publicidad, la funcionalidad y el buen servicio convirtió al 12 de diciembre del mismo año como el día con mayor transacciones móviles gestionando de esta manera $4.700.000 dólares. (Historia. 2013. PayPal. 01 Abril 2014. https://www.paypal-media.com/es/history).

En el año 2011, PayPal firmó un acuerdo con "Caixa (Caja de Ahorros y Pensiones)" aceptando a la entidad como medio de pago para sus ventas en Internet (Historia. 2013. PayPal. 01 Abril 2014. https://www.paypal-media.com/es/history); además integra en su plataforma de banca electrónica, Línea Abierta, de manera que todos los clientes de la Caixa puedan abrir gratis y cómodamente una cuenta, posterior a ello se lanzó una tarjeta de crédito PayPal que servía para pagos en cualquier tienda que tuviese convenios con PayPal o tarjetas Visa de esta forma se consiguió hasta un 2% de bonificación; con el pasar del tiempo PayPal creció cinco veces más que en el año 2010; es por eso que en el 2012 generan aplicaciones para mejorar la eficacia de PayPal (Historia. 2013. PayPal. 01 Abril 2014. https://www.paypal-media.com/es/history), permitiendo realizar compras incluso cuando la tienda este cerrada, es decir dejando acceder a los usuarios al catálogo de la misma, aprobando las transacciones en tiempo real; además PayPal acordó con 15 conocidas firmas: Abercrombie & Fitch, Advance Auto Parts, Aéropostale,

American Eagle Outfitters, Footlocker, Guitar Center, Jamba Juice, JC Penney, Jos. A. Bank Clothiers, Office Depot, Rooms to Go and Tiger Direct, Toys R Us.

PayPal pretendió llegar en el año 2013 a 20.000 millones de dólares en pagos realizados desde dispositivos móviles; conforme avanzó el sistema tecnológico dentro de PayPal se lanzó "PayPal Here" versión chip PIN (Historia. 2013. PayPal. 01 Abril 2014. https://www.paypal-media.com/es/history)la cual fue diseñada con el objetivo de ser empleada en las tiendas de países que se basan en tecnologías chip y pin; por ultimo PayPal lanzó una tarjeta prepago con flexibilidad para los pagos, ya que no necesita estar vinculada a una cuenta bancaria, simplemente tiene la opción de recargarla.

Cabe recalcar que eBay y PayPal son independientes, es decir, a pesar de que las cuentas funcionan de manera conjunta, se gestionan por separado. Algunas actividades sólo realizan con PayPal.

4.1.1.1 Definición y funcionamiento

4.1.1.1.1 Definición:

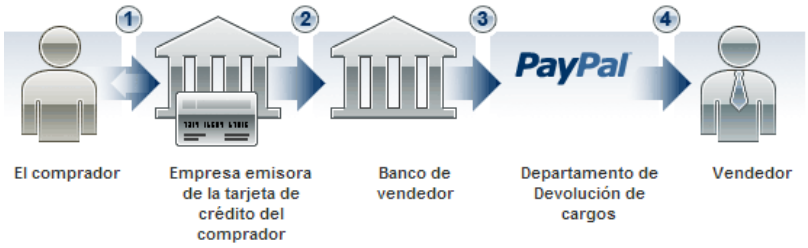
PayPal es una forma de pago de la casa de eBay, el cual brinda facilidad a los compradores y vendedores por Internet, a las pequeñas empresas; ya que permite enviar y recibir pagos de forma más sencilla, gratuita y en línea sin tener que compartir información, en más de 190 países, los mismos que afirman que *"Paypal te permite enviar pagos de forma rápida y segura a través de Internet mediante una tarjeta de crédito o cuenta bancaria."* (Formas de Pago. 2014. PayPal. 01 Abril 2014. http://pages.ebay.es/help/pay/methods.html#paypal). Ésta es una de los principales redes de pagos para sitios Web, el mismo que fue iniciado para subastas y poco a poco se ha introducido en otros negocios electrónicos como la venta de

artículos y diversos servicios, ayudando a sus usuarios en las diversas transacciones convirtiéndose en la compañía con mayor crecimiento del comercio móvil según la organización "Meet Magento" de España, quien indica que procesó 27 mil millones de dólares en pagos móviles, en el año 2013(Transacciones PayPal.2013.PayPal. 01 Abril 2014. http://es.meet-magento.com/paypal). Para que los usuarios puedan pagar por los productos o servicios adquiridos, deben tener una cuenta de correo electrónico, y la pueden utilizar desde cualquier computadora personal o teléfonos inteligentes que posean Internet, ya que de ésta manera podrán enviar y recibir información. "*La red de PayPal se basa en la infraestructura financiera existente de cuentas bancarias* y tarjetas de crédito para crear una solución global de pago en tiempo real." (Elegir una forma de pago. 2014. Ebay. 02/Abril/2014 http://pages.ebay.es/help/pay/methods.html#paypal), al cual se le puede realizar un seguimiento desde la cuenta de PayPal del consumidor.

Una de las grandes ventajas que ofrece PayPal es que al momento de realizar el pago los vendedores no podrán observar el número de tarjeta, ya que éste se cifra de forma segura, además que el dinero se deposita automáticamente en la cuenta del mismo, sin intermediarios, ni necesidad de terceros, limitando el riesgo de uso no autorizado; cuidando de esa manera la información de las amenazas externas; pues de ésta manera Paypal puede confirmar y cumplir con su "promesa de seguridad", la misma que asegura confidencialidad e integridad de la información personal y

Figura 32. Seguridad de la Información (https://www.paypal.com/ec/webapps/mpp/paypal-safety-and-security)

Además tiene una política denominada "Protección del comprador de PayPal", la misma que contiene requisitos indispensables que debe cumplir el comprador en caso de querer reclamar si el producto no es el requerido o tiene algún desperfecto que debe ser reportado en un lapso de 60 días aproximadamente, para proseguir con reembolsos parciales o totales, según sea el caso; realizándose dichas acciones de la siguiente manera:



1. El comprador solicita la devolución del cargo de la empresa emisora de la tarjeta de crédito.
2. La empresa emisora de la tarjeta de crédito del comprador notifica al banco vendedor de PayPal el contracargo y carga los fondos a PayPal.
3. PayPal retiene temporalmente los fondos relacionados con el contracargo en la cuenta PayPal del vendedor.
4. PayPal envía inmediatamente un correo electrónico al vendedor para pedirle información adicional que se puede utilizar para impugnar la devolución de cargo.

Figura 33. Protección al comprador de PayPal (https://www.paypal.com/ec/webapps/mpp/security/sell-chargebackguide1)

4.1.1.1.2 Funcionamiento:

Figura 34. Funcionamiento PayPal (https://www.paypal.com/ec/webapps/mpp/consumer-how-paypal-works)

Como ya se mencionó anteriormente, una de las formas más rápidas de pagar y cobrar por transacciones realizadas en línea, es hacerlo mediante Paypal, para ello es

necesario conocer los procesos que debe seguir el tarjetahabiente al momento de registrarse y de utilizar correctamente los beneficios que brinda éste; existen dos procedimientos principales, los mismos que son:

1. Apertura de la Cuenta.
    a. Registrarse. Para realizar éste procedimiento el usuario debe llenar un formulario electrónico de registro, donde se identificará como persona natural o jurídica y enviará los datos; a la vez que recibirá un vínculo de confirmación de correo electrónico. Cabe recalcar que éste proceso es sin costo alguno.
    b. Asociar Tarjeta de Crédito. El usuario tiene una gran ventaja, pues podrá asociar a su cuenta Paypal una o varias tarjetas de crédito, las mismas que quedarán almacenadas para las próximas compras.

Es decir, el tarjetahabiente brinda todos los datos requeridos por Paypal para crear su cuenta y por otra parte Paypal almacena toda la información brindada de forma segura, protegiéndola de fraudes internos o externos, de ésta manera el usuario podrá realizar compras futuras.

1. Pago. El usuario tiene la ventaja de pagar en línea, Paypal retira el importe de pago de la tarjeta que ha elegido para realizar la compra y transfiere el dinero al negocio electrónico sin necesidad de intermediarios, de la siguiente manera:
    a. Una vez escogido los productos del portal web, se debe elegir el botón de Paypal para realizar la compra, y se inicia sesión ingresando la

dirección de correo electrónico como usuario y la contraseña correspondiente.

Figura 35. Login de Compra Paypal (https://www.paypal.com/ec/webapps/mpp/paying-with-paypal)

b. El comprador no deberá ingresar información de la tarjeta, solo confirmar la compra, e inmediatamente se realizará la transacción.

4.1.1.2 Políticas

Estos acuerdos son de mutuo consentimiento pues están a libre elección de aceptar o no los términos de uso de la herramienta y/o servicios que brinda la entidad; además es necesario tener políticas como respaldo para ambas partes es decir, por un lado los usuarios aceptarán los términos y condiciones para empezar a utilizar el servicio haciéndose responsables de la aprobación de los mismos, por otro lado la empresa muestra al usuario final la información detallada del funcionamiento y procesos de la tienda dando mayor confianza, certeza y credibilidad a los interesados.

Ver Términos de Referencia entre el Usuario y PayPal: *https://cms.paypal.com/es/cgi-bin/marketingweb?cmd=_render-content&content_ID=ua/BuyerProtection_full&locale.x=es_ES*.

4.1.1.3 Costos

Una de las grandes ventajas con las que cuenta PayPal es que se la podría llamar "intermediario" pues permite realizar transacciones con diferentes tarjetas de crédito o débito, funcionando como juez entre compradores y vendedores, garantizando que el pago por compras de bienes o servicios, y las transacciones realizadas, sean realizadas con seguridad y rapidez; contando con tasas más bajas a comparación de otras entidades financieras. Los costos por transacciones personales (envío y recepción de dinero) ya sean nacionales o internacionales y por transacciones comerciales se detallan en el siguiente enlace:

https://cms.paypal.com/es/cgi-bin/?cmd=_render-content&content_ID=ua/ES_20100121_Amendment_to_UA_AND_PRIVACYPOLICY_print.

PayPal no cobra tarifas adicionales al valor a pagar del bien o servicio, si es que no existe conversión de divisas.

En el caso del vendedor, persona natural o jurídica que recibe los pagos, deberá cancelar un porcentaje del 3.4 % + la tarifa por conversión de divisas, a menos que sea un vendedor mayorista, es decir que previa aprobación de PayPal a una solicitud emitida por el mismo, en el que se consideran, volúmenes mensuales de ventas, cuentas sin irregularidades, cantidad promedio de ventas, tendrá una tarifa que oscila entre el 1.9% al 2.9% más tarifa de divisas.

Las tarifas fijas que se suman a los pagos realizados con tarjeta de débito o crédito son basados en los impuestos a las divisas que cobra PayPal, y éstos dependen del país en el que se haga la transacción. *https://www.paypal.com/es/webapps/mpp/ua/privacy-full*.

4.1.2 Visa

Visa es una compañía de tecnología, una red comercial que facilita el comercio global, pues conecta a instituciones financieras, comercios, consumidores, compañías, entidades gubernamentales y permite pagos electrónicos, programas de crédito, débito, prepago y acceso a efectivo.

Visa maneja aproximadamente "*20.000 transacciones por segundo*" (Verified by Visa. 2014. Visa. 28 Abril 2014. http://lac.visa.com/consumers/security.jsp), con fiabilidad y comodidad, además de la seguridad que brinda con su tecnología denominada Verified by Visa, la misma que ofrece protección contra fraudes a los consumidores y pago garantizado a los comercios.

4.1.2.1 Definición y funcionamiento

4.1.2.1.1 Definición:

Verified by Visa, es el nuevo servicio de autenticación On Line de Visa, el mismo que permite que el e-commerce sea seguro, pues brinda protección a los datos y transacciones del cliente, ya que al momento de comprar en línea, éste debe añadir a la tarjeta Visa una contraseña personal, y así ser identificado en tiempo real; logrando de ésta manera combatir las actividades fraudulentas y limitar los riesgos.

Verified by Visa tiene principalmente dos pilares fundamentales; el primero, es dirigido hacia los comerciantes, pues ellos buscan construir y mantener su canal de comercio electrónico, y al contar con este servicio, demuestran solidez, rectitud en los negocios y garantizan seguridad a los tarjetahabientes; mientras q el segundo es esencial para el usuario, porque éstos son los que requieren un servicio fácil, sencillo pero que les brinde la confianza requerida.

Algunas de las ventajas y beneficios que brinda el servicio de Verified by Visa son:

- Aumento de la seguridad en las transacciones.
- Incremento de la satisfacción del cliente.
- Impulsará las ventas en el comercio electrónico.
- Mejoramiento de la rentabilidad de los negocios electrónicos
- Manejo de cargos operacionales reducidos.
- Uso de herramientas automatizadas.
- Reducción de las devoluciones fraudulentas.
- Aumento de la confianza del titular de la tarjeta
- Es un servicio de fácil integración en e-commerce existentes.
- Brinda garantía de pago.
- Protección para el uso no autorizado de las tarjetas.
- Es de uso Fácil, pues no requiere de ningún software especial para computadoras.

(Ventajas Verified by Visa. 2014. Visa Europe. 3 mayo 2014. http://www.visaeurope.es/su-tarjeta-visa/compre-en-internet-verified-by-visa/ventajas)

4.1.2.1.2 Funcionamiento:

Cuando un cliente ha escogido los productos y/o servicios que requiere, y ha terminado de llenar el carrito de compras, da el respectivo clic en el botón de [Enviar o Comprar] para confirmar la orden; en ese momento recibe una alerta de Visa, indicando una de las siguientes situaciones:

- Si es que el tarjetahabiente no contrata aún el servicio del PIN para Verified by Visa, se notifica a los titulares de tarjetas que debe activar su tarjeta para Verified by Visa.

- En caso de ser usuarios de Verified by Visa, se pide a los mismos proporcionar la contraseña.

En ambas situaciones el sistema enviará una alerta donde se pide de favor a los usuarios esperar mientras la transacción está siendo procesada y no hacer clic en el "Botón de atrás", o en el ícono de cerrar ventana, ya que al realizar éstas acciones los procedimientos se interrumpen y las operaciones de compra no se concluyen con éxito.

4.1.2.1.2.1 Procedimiento de activación

4.1.2.1.2.1.1 Activación

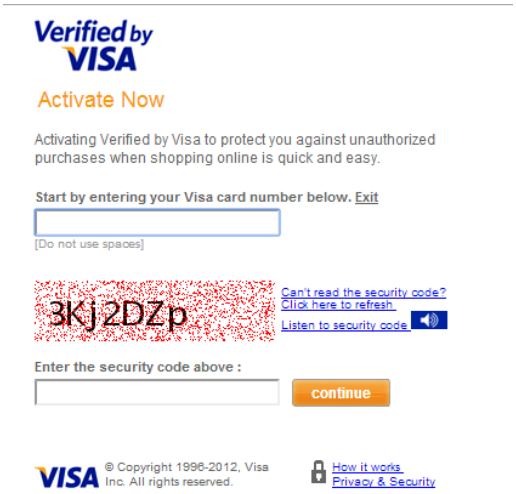


Figura 36. Activación. (http://www.visa.com.ar/socios_seguridad-proteccion.aspx)

Para que se realice el proceso de activación, el usuario debe ingresar el número de la tarjeta Visa en un formulario como el de la figura anterior, en ese momento el sistema confirmará el mismo y presentará la página que se acomode al caso, es decir, si es que el titular de dicha tarjeta está activo en el servicio de Verified by Visa, se mostrará la página denominada "activación emisor", caso contrario la de "inscripción emisor".

4.1.2.1.2.1.2 Verificar identidad y activar

Una vez que el cliente ingresa el número de tarjeta, existe un procedimiento que ejecuta el servidor de activación para comprobar si es que el número de la tarjeta Visa es válida, en caso de que si lo sea, el portal web puede solicitar información del tarjetahabiente para autenticar al titular de la tarjeta, de la siguiente manera:

Se debe ingresar los 4 últimos dígitos de la tarjeta, el código CVV y la fecha de nacimiento del tarjetahabiente, en algunos casos se pedirá también un email, de ésta forma se verificarán datos de identidad y en caso de ser todos correctos, el proceso de activación terminará con éxito.

Figura 37. Verificación de Datos (http://www.visa.com.ar/socios_seguridad-proteccion.aspx)

4.1.2.1.2.1.3 Crear contraseña

Una vez autentificado el usuario, éste debe crear una contraseña difícil de adivinar y segura, para poder utilizarla cuando realice transacciones On Line:

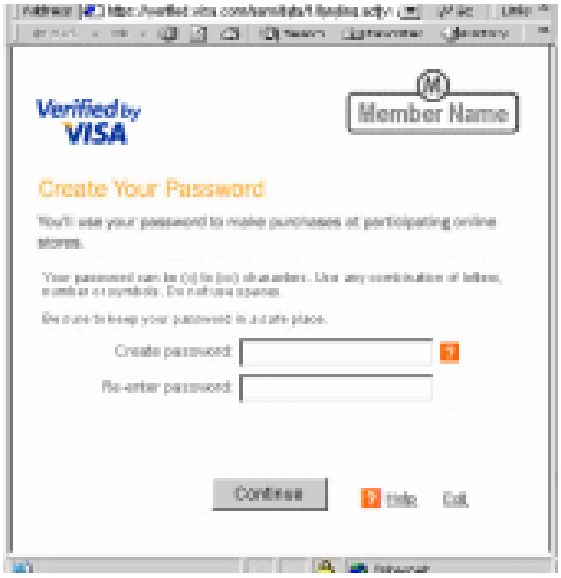


Figura 38. Contraseña: (http://www.visa.com.ar/socios_seguridad-proteccion.aspx)

4.1.2.1.2.1.4 Confirmar la Activación

Una vez realizada la activación, se muestra una página indicando el éxito de la activación al tarjetahabiente, la misma que es:

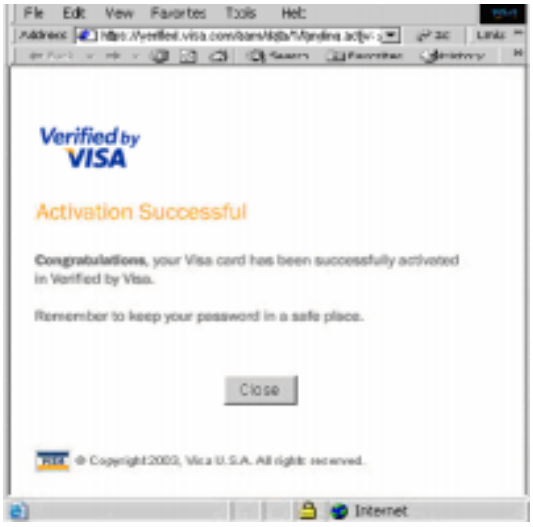


Figura 39 Mensaje se Activación Satisfactoria. (http://www.visa.com.ar/socios_seguridad-proteccion.aspx)

En ese momento el usuario debe hacer clic en el botón Cerrar, y enseguida se re direcciona a la página de la tienda virtual.

Una vez realizado el proceso de activación, el cliente puede realizar cualquier tipo de transacción en negocios en línea, simplemente utilizando el número de tarjeta y su contraseña. Verified by Visa es una capa adicional de seguridad, suministrado por Visa, para brindar tranquilidad a los compradores en línea.

4.1.2.1.2.2 Procedimiento de compra

Después que el usuario registró su tarjeta en Verified by Visa, y eligió ya su contraseña y el mensaje personal con el que va a quedar inscrito, compra en cualquier negocio electrónico que participe en verified y al momento de completar la compra y hacer clic en el botón de pagar:

1. Ingresa el número de tarjeta Visa
2. Escribe la contraseña de Verified by Visa
3. Aparece el mensaje de que la compra fue completada con éxito y regresa a la página del portal web.

Figura 40 Procedimiento de Compra (http://www.visa.com.ar/socios_seguridad-proteccion.aspx)

4.1.2.2 Políticas

La entidad financiera Visa se dedica a la transferencia de información y datos importantes entre diversas instituciones, las mismas que pueden ser financieras, comerciales, gubernamentales, etc. Es por ello que éste organismo explica en su sitio web la política de privacidad: "Visa está comprometida a proteger su privacidad. Visa ("nosotros", "nos" o "nuestro/a(s)") protege su información personal para mantener la confianza del consumidor."(Política de privacidad de Visa.2014. Visa. 15 mayo del 2014 http://lac.visa.com/about/privacy.jsp)

4.1.2.3 Costos

Una de las grandes ventajas que se tiene al comprar en línea es la facilidad de pago, es por ello que las personas que comercializan por la web eligen diferentes métodos y maneras para realizar el mismo, siendo uno de estos el pago con tarjeta Visa, bajo la seguridad de Verified, el mismo que tiene como Visión "permitir pagar y recibir pagos de forma cómoda y segura, cuando quieras, donde quieras, y con cualquier dispositivo". Es por eso que muchos de los comercios eligen que sus transacciones sean realizadas mediante esta tarjeta, siendo los costos los siguientes:

- Compras al contado con tarjeta de crédito: 4%
- Compras al contado con tarjeta de débito: 2,6%
- Compras diferidas, oscilan entre un 5 a 10% dependiendo del valor y plazo al cual se difiera.

Cabe recalcar que el tarjetahabiente deberá cancelar un extra por el impuesto a la salida de divisas, dependiendo del país en el que se encuentre y en el que se haga la compra.

4.1.3 MasterCard

MasterCard tiene como objetivo transformar a las empresas en líderes del comercio electrónico, además de ayudarlas a crecer y prosperar, cabe recalcar que es una de las tres tarjetas más importantes dentro de los vendedores de todo el mundo, esta entidad es una marca de tarjetas de crédito y de débito de mayor confianza para los clientes pues utiliza como medida de seguridad un número PIN denominado "CódigoSeguro o SecureCode"; tener una tarjeta es conveniente además de una necesidad, ya que se puede realizar compras en más de 24 millones de lugares alrededor del mundo.

4.1.3.1 Tarjetas MasterCard:

Existen varios tipos de tarjetas MasterCard, cada una con diferentes beneficios, requisitos y servicios. (Tipos MasterCard. 2014. MasterCard. 14 enero 2014, http://www.pacificard.com.ec/mastercard/tipos.aspx)

4.1.3.2 Definición y Funcionamiento

4.1.3.2.1 Definición:

MasterCard SecureCode es un servicio tecnológico que incluye un código privado que solamente será de conocimiento para dueño de la tarjeta y el banco al que pertenece; además representa un mayor grado de protección contra el uso prohibido de la tarjeta, es decir, cuando ésta no está autorizada para realizar compras en tiendas online; una vez que el usuario obtenga su SecureCode protegerá su cuenta de robos informáticos.

4.1.3.2.2 Funcionamiento:

Los pasos para el funcionamiento del SecureCode son:

4.1.3.2.2.1 Ingresar a la tienda virtual:

Figura 41. Ingreso Tienda Virtual (http://www.pacificard.com.ec/)

4.1.3.2.2.2 Registro:

Para registrarse aparecerá una ventana de MasterCard Secure Code, en donde se deberá ingresar los datos del tarjetahabiente.

Figura 42. Ingreso de Datos Tarjetahabiente (http://www.pacificard.com.ec/).

4.1.3.2.2.3 Creación de Código de Seguridad:

Se creará el código de seguridad, el mismo que no se deberá compartir con terceras personas, para mayor seguridad la clave se debería ser memorizada.

Figura 43. Creación de Código de Seguridad (http://www.pacificard.com.ec/)

4.1.3.2.2.4 Compra realizada:

Una vez obtenido el código de seguridad, se continuará con el proceso normal de la compra.

Figura 44. Mensaje de Aviso (http://www.pacificard.com.ec/)

4.1.3.2.2.5 Verificación del Código de Seguridad:

En caso de que el usuario posea un código de seguridad (SecureCode), la tienda virtual solicitará la digitalización del código de seguridad mientras se realiza

el proceso de pago, la institución financiera realizará el proceso de validación del SecureCode de una manera rápida y segura para que se pueda concluir la compra. El SecureCode no será compartido con el comercio, ya que equivale al ingreso del PIN de seguridad en un cajero automático (ATM).

Figura 45. Ingreso del Código de Seguridad (http://www.pacificard.com.ec/)

En caso de que el SecureCode sea incorrecto, la compra no se efectuará; cabe recalcar que si una persona supiera el número de la tarjeta de crédito o débito, la compra no puede concluirse sin el SecureCode digitado en la tienda. El código de seguridad o SecureCode de MasterCard tiene la ventaja de ser compatible con la mayoría de navegadores.

4.1.3.3 Políticas

MasterCard SecureCode crea lineamientos que seguirán un proceso de tareas y reglamentos para cumplir las metas propuestas por la entidad, de manera que solo se podrá utilizar el servicio y realizar transacciones siempre y cuando haya una aprobación de las partes de cada uno de los términos. (*Términos de Uso. 2011. MasterCard. 25 Febrero 2014.* *https://www.bncr.fi.cr/BNCR/BNSecure/PDF/BNCR%20-%20BN%20Secure%20-%20Terminos%20y%20condiciones%20MCSC.pdf*).

4.1.3.4 Costos

El interés en compras por internet tienen el mismo valor que las compras físicas, el cual se calcula tomando la tasa representativa que se encuentre al momento en el banco en el que la tarjeta este asociada; para este año (2014) la tarifa de las transacciones que se realizan con tarjeta de crédito está comprendida entre un 3 a 4 porciento, por otro lado con tarjetas de débito existe un interés del 2,6%(DataFast Ecuador. 2014); suele cobrarse además un porcentaje por el riesgo que corre la empresa a estafas virtuales.

CAPITULO 5. Análisis comparativo Costo-Beneficio entre PayPal, Visa, MasterCard

5.1 Evaluación de las formas de pago de cada una de las empresas emisoras de las tarjetas de Crédito.

Las empresas emisoras de las tarjetas de crédito son entidades con políticas establecidas, las mismas que se encargan de brindar seguridad, confiabilidad, facilidad de uso, al momento de que el tarjetahabiente realice una transacción; sin embargo por el servicio que prestan reciben remuneraciones y porcentajes establecidos dependiendo del movimiento bancario, el lugar en el que se efectúe y el bien o servicio a brindar.

5.1.1 Análisis Costo Beneficio

La implementación del carrito de compras en un comercio electrónico trae consigo muchos pros y contras que deben ser identificados, pues el correcto análisis de los mismos que permitirá conocer costos estimados y los beneficios que significaría para el e-commerce contar con dicho servicio.

Algunos de los factores determinantes que intervienen en éste proceso son:

5.1.1.1 Costo Mano de Obra

La mano de obra es un factor muy importante pues representa el monto del coste total de los trabajadores que tenga la empresa, en donde se incluye el sueldo y cualquier tipo de impuestos que se encuentren ligados a ellos; tanto la correcta administración como el adecuado control podrán determinar el costo final ya sea del producto o servicio que brinda la organización. Para la definición respectiva del valor total es necesario separar los tipos de mano de obra:

Mano de Obra Directa: Conocida también como manos de obra de toque, se refiere al trabajo que realiza directamente el empleado el mismo que es responsable de fabricar el producto.

- Mono de Obra Indirecta: Es todo aquel o aquello que no tenga contacto directo con la fabricación del producto, es decir apoya a la producción mas no elabora o implementa el producto.
- Mano de Obra de Gestión: Esta función corresponde a los directivos y ejecutivos que pertenecen a la empresa.
- Mano de Obra Comercial: Es el trabajo generado por el área comercial la misma que es fundamental para la empresa.

La mano de obra radica en que es un factor importante ya que elabora con excelencia y calidad los productos o servicios que ofrece la empresa.

5.1.1.2 Costos Administrativos

Se refiere a los gastos o costos que se aplica en la elaboración de trámites y movimientos dentro de la empresa, los mismos que son manejados por los gerentes y administradores; siendo generados básicamente por sueldos de gerentes, administradores, y demás personal, quienes no influyen directamente con la elaboración de la producción. En el comercio electrónico hay una significativa reducción de personal, ya que existe el software automatizado el cual realiza todo el proceso de compra online, es decir generan de manera mecánica las transacciones y recibos, razón por la cual la empresa reduce personal pero mejora sus ganancias.

5.1.1.3 Consideraciones

Los clientes que compran en sitios web no presentan de manera física la tarjeta de crédito al momento de cancelar la orden, las transacciones que se realizasen en línea tienden a mayor riesgo de fraude informático es por eso que los procesadores de pago cobran un porcentaje como comisión por cada transacción, estas son más altas que las que se fijan para las tiendas físicas. Cuando se tiene comercio electrónico es posible que la tienda deba pagar cargos como la puerta de entrada de Internet, costos de reserva, entre otros.

5.1.1.4 Instalaciones

Una tienda física requiere de infraestructura, además de pagos de impuesto, pagos de servicios básicos, personal de venta, etc.; por otro lado la tienda virtual necesita de un servidor, dominio, enlaces de internet, proveedores de internet, unidades de respaldo, un portal web, la entidad de pago, certificado digital, publicidad, además del software del carrito de compras y el botón de pago. Se debe considerar si es necesaria la creación de una tienda virtual implementado el software o si es conveniente alquilar a entidades que ya poseen este tipo de servicio. En el siguiente cuadro se detallarán los costos de inversión que tendrán las empresas que deseen montar una tienda electrónica.

Descripción	Costos Aproximados
Software	$110000
Hardware	$ 20000
Personal	$ 8000

Tabla 7. Instalaciones. Fuente: www.livecommerce.es. Consultoría y desarrollo e-commerce

5.1.1.5 Eficiencia

Se puede decir que un proceso es eficiente cuando se aprovecha al máximo cada recurso con el que se pueda contar, disminuyendo de ésta manera los costos de producción; tomando en cuenta dicha definición, se puede hacer una analogía con la realidad, pues uno de los más grandes recursos que se tiene es la tecnología, es por ello que si los negocios utilizan dicha fortaleza aumentarán su eficiencia.

Según un artículo publicado por la IRC (Internet Resource Center) de la Southeastern Louisiana University *"la naturaleza automatizada del comercio electrónico puede automatizar el inventario y notificar al propietario de la empresa cuando los suministros, si hay disponibles, se convierten en baja. Los sitios de comercio electrónico también pueden automatizar los pedidos y la gestión de relaciones con vendedores y proveedores y los sitios crean una interfaz pública consistente para clientes…"*. Es decir, como ya no existe la intervención de un individuo en la toma de decisiones al momento de procesar pedidos, sino que los procesos del carrito de compras lo automatizarán, será un método más eficiente y por lo tanto reducirá costos.

5.1.1.6 Marketing y Publicidad

Al momento que se toma la decisión de implementar un negocio electrónico, hay que tener en cuenta que una buena estrategia es el marketing en línea, el cual hace referencia a la mercadotecnia que se realizará por internet para el posicionamiento de la empresa en la Red, es decir ponerse en contacto con el mercado meta, informarles sobre productos, promociones, a través del correo electrónico, buscadores, redes sociales, etc.; incrementando de ésta manera estímulos en la gente para motivarlos a comprar o adquirir un servicio.

La Publicidad en este tipo de comercios tiene un papel trascendental pues, si un portal web no es conocido, no tendrá consumidores; así que es importante gastar un capital alto en una estrategia de marketing que a corto plazo se convertirá en

ganancias, por lo que más que un gasto es una inversión. Además que el marketing en línea es menos costoso que el tradicional y brinda ventajas vitales como un mayor alcance y flexibilidad para realizar algún tipo de cambios.

Costos Marketing anual	Tendencia
100 000 dólares	Aumentar aproximadamente un 20% al año.

Tabla 8. Marketing y Publicidad. Fuente1: www.livecommerce.es. Consultoría y desarrollo e-commerce Fuente2: Mirasol S.A. Departamento de Marketing.

Los factores antes explicados se pueden identificar como requerimientos esenciales para la correcta implementación de un sistema de e-Commerce, los mismos que son sintetizados a continuación:

Requerimientos	Descripción		
	Del servidor Web	Tiene que ser simple, pero muy estable, rápido y debe adaptarse fácilmente a diversas tecnologías, plataformas y protocolos.	• Apache • Tomcat • Cherokee • Internet Information Server (IIS)
		La característica principal que éste debe brindar es la	

Software	Sistema Operativo	estabilidad, accesibilidad y por supuesto seguridad, pero se debe tener cuidado si éste software será soportado por el hardware.	• Centos • Ubuntu • Windows • MAC
	Para crear el Sitio Web	Debe tener una implementación sencilla, con un atractivo diseño visual e interface amigable, permitir personalizar el Sitio web y no tener costes demasiado altos, además de no consumir muchos recursos y cumplir con los requerimientos del servidor.	• Magento • Opencart • Oscommerce • Prestashop
		Deben tener buen rendimiento en la	• Oracle • Sql Server

	Base de Datos	parte transaccional, poseer velocidad en tiempos de respuesta, además de seguridad, integridad y confiabilidad.	• DB2 • Postgre-SQL
	De Seguridad	Brinda seguridad y confiabilidad a los usuarios.	• VeriSign • Norton Secured
Hardware	Para hospedar el Software	Las características que deben cumplir éstos equipos con de brindar mayor procesamiento y rapidez, ahorrando energía, tiempo.	• Servidores • Unidades de respaldo • PC's • Instalaciones
Publicidad	Marketing	Debe contener estímulos visuales, tener una redacción que impulse la compra, ser intuitiva, sencilla y llamativa.	• Banners • Push adversting • Webspots

Humano		Para la implementación del portal web, se requiere de expertos en las diferentes disciplinas que sean responsables, éticos y comprometidos.	• Gerente (dueño de la tienda) • Desarrollador • Publicista • Experto en redes • Especialista de sistemas de información para mantener el sitio.
Otros	Internet	Debe ser un servicio que brinde una empresa sólida y responsable, que ofrezca un ancho de banda rentable.	• Comercial • Avanzado
		Es necesario que para la creación de un portal web, se realice un análisis externo en ámbitos	• Outsourcing con una empresa seria,

	Consultoría	como la gestión comercial, de la información, de ésta manera se puedan disminuir las ineficiencias en cada uno de los procesos que deba desarrollar el comercio.	responsable y con criterios amplios. • QA. Garantía de Calidad.

Tabla 9. Requerimientos. Elaboración: Autoras, Cuenca – Ecuador 2014.

5.1.2 Ventajas y Desventajas

Claro está que cada uno de los recursos humanos y materiales que se requieren para la implementación del carrito de compras en un comercio, tienen costos elevados, como se explicó en los cuadros anteriores; sin embargo trae consigo múltiples beneficios, pues al tener tan grande ventaja competitiva, su mercado sería cada vez más amplio, pues ganaría clientes con la presencia del portal en la web. Entre otros beneficios se puede rescatar los siguientes:

- Ampliar el mercado con la captación de más clientes, pues la empresa se conocerá mundialmente.
- La innovación, ya que si el portal web se mantiene actualizado, brindará mayor confianza a los clientes para que realicen sus transacciones.

- Si es que los clientes pueden comprar sin ningún recelo en los portales web, obviamente aumentará las ventas, pues a mayor confianza, mayor rentabilidad.
- Mejora en la toma de decisiones.
- Facilidad en cobros y pagos, ya que podrá realizarse dichas transacciones, cualquier día del año, a la hora que el cliente lo desee.
- Los clientes optimizarán tiempo y dinero, pues para realizar una reservación o compra, no necesitan trasladarse a las tiendas a comparar opciones, solo requieren de internet, y los productos adquiridos los recibirá en un lugar elegido por el usuario.

Reducción de costos, porque el dueño de la empresa, no tendrá que cancelar un valor por la tienda física, servicios básicos; también se reduciría el pago de sueldos a empleados, ya que no se necesita de una persona que constantemente atienda la tienda

5.1.3 Conclusiones

Una tienda que cuente con el servicio de compra en línea, tiene todos los beneficios explicados anteriormente, lo que le da una gran ventaja competitiva llamada “eficiencia”, y es muy importante que un portal web cuente con éste, ya que de dicha manera brinda un mayor grado de confiabilidad a los clientes, pues vivimos en una sociedad donde las personas son cada vez más exigentes, informados y equipados con tecnología de punta para realizar compras, comparar precios, buscar información detallada sobre ciertos productos y las tiendas que los comercializan, por lo que los negocios deben buscar nuevas formas de mantener sus ventas y sus clientes.

En la actualidad las empresas que tienen más éxito son las que se enfocan a cubrir necesidades comerciales, a estudiar e investigar formas para brindar un mejor y renovado servicio a través de la tecnología, según Guillermo Cevallos, un exitoso director de Desarrollo de Negocios de Retail de Motorola Solutions México, en un artículo publicado en ComputerWorld Ecuador afirma: *"el e-commerce puede ser la llave para relanzar un negocio tradicional o iniciar un nuevo proyecto*, *maximizando las oportunidades que nos ofrece la Era Digital"*(ComputerWorld. 2014. Era Digital. 12 Mayo 2014).

La evolución de la tecnología y el incremento del mercado potencialmente activo exigen a los comercios seguir a la vanguardia de las necesidades de los consumidores, pues de dicha manera no solo éstos tendrán satisfacción, sino que el mismo e-Commerce será beneficiado con el incremento de clientes, aumento de ventas y por lo tanto mayor remuneración económica; concluyendo de ésta manera que la inversión que se debe realizar a un negocio tradicional para convertirlo en uno virtual o la iniciación del mismo, será muy rentable, según la Secretaría Nacional de Telecomunicaciones.

Ver e-commerce Ecuador Actual (e-commerce Ecuador actual. El Comercio Electrónico en el Ecuador Actual. 2014. Ministerio de Telecomunicaciones del Ecuador. 10 de Junio 2014. http://www.telecomunicaciones.gob.ec/).

5.2 Análisis de la seguridad mediante modelo de calidad ISO 25001

La Organización Internacional de Estándares (ISO), ha definido un conjunto de reglas y procedimientos que se deben seguir en la elaboración de un producto o servicio, para que éste pueda ser aprobado y satisfaga los estándares de calidad; cabe recalcar que al hablar de calidad se hace alusión a cada una de las cualidades de un

producto o servicio para satisfacer las distintas necesidades de los usuarios; en éste caso se hará referencia a que los productos software también tienen que cumplir con requisitos y especificaciones para alcanzar la calidad deseada; Roger Pressman afirma que " *La calidad de concordancia es el grado de cumplimiento de las especificaciones de diseño durante su realización…. cuanto mayor sea el grado de cumplimento, más alto será el nivel de calidad de concordancia.*"

Para "medir" la calidad de un software se crearon varias ISO, dentro de las cuales se encuentra la ISO 25010, la que será objeto de esta investigación.

Figura 46. Calidad del Producto Software. ISO 25010 (ISO/IEC 25010. 2014. ISO 25000 Calidad del producto Software. 28 Mayo 2014. http://iso25000.com/index.php/normas-iso-25000/iso-25010)

Éste modelo establece características que deben ser usados al momento de evaluar el producto software, las mismas que son: Adecuación Funcional, Eficiencia de desempeño, Complejidad, Usabilidad, Fiabilidad, Seguridad, Administrabilidad y Portabilidad; cada una de las cuales tiene sub características, dependiendo de los parámetros que se desea alcanzar.

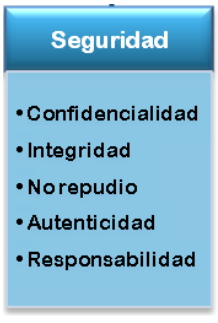


Figura 47. Seguridad. ISO 25010 (ISO/IEC 25010. 2014. ISO 25000 Calidad del producto Software. 28 Mayo 2014. http://iso25000.com/index.php/normas-iso-25000/iso-25010)

En ésta investigación se hará referencia únicamente a la característica de: “Seguridad”, la misma que se entiende como la capacidad que tiene cada software para proporcionar protección a la información personal y financiera de una persona o empresa, cuidando su integridad y evitando que la misma sea modificada por terceros, amenazada o que sufra algún fraude; tomando en cuenta la infraestructura, los servicios que brinda, los protocolos de seguridad con los que va contar.

Se conoce que para salvaguardar la información se requiere de un buen capital, pero hay que tomar en cuenta que no sería un gasto, sino una inversión, pues mientras más seguro sea el software más aceptación tendrá en el mercado, pues minimizará riesgos aumentando confiabilidad en los clientes y todo el dinero invertido, se podrá recuperar en un corto lapso de tiempo.

Dicha característica se compone a su vez de cinco subcaracterísticas que deberán ser cumplidas a cabalidad para poder cumplir con la calidad de software deseada:

5.2.1 Confidencialidad

Esta característica hace referencia a la capacidad que tiene el sistema para proteger la información personal y financiera de los usuarios, es decir que la misma no sea visible, ni accesible para terceros no autorizados, dando de ésta manera confianza a los clientes para que puedan depositar sus datos a quienes cuenten con dicha característica.

Según la ISO 25010, la confidencialidad es "*garantizar que la información sea accesible sólo para aquellos autorizados a tener acceso…*". Es decir solo la

persona dueña de la información puede elegir con quien desea compartirla y de forma parcial o total.

Pero a ésta característica se le debe atribuir una excepción, pues en el caso que hubiere algún tipo de incumplimiento de la ley, o se requiera dicha información necesaria para emprender una acción legal en contra de algún individuo que incumpla con los términos y condiciones que presente la Institución dueña del software, se debe recurrir a alguna autoridad que siga legalmente los procesos pertinentes.

5.2.2 Integridad

Dentro de los sistemas electrónicos la integridad es un punto muy importante pues hace referencia a la capacidad que poseen los sistemas para controlar los accesos o modificaciones a la información que no estén autorizados; además se puede verificar la manera en que se resiste a los ataques (tanto accidentales como intencionales) contra la seguridad. El ataque puede dañar al programa, datos y documentos.

La integridad valida al mensaje aplicándole una función criptográfica a los datos es decir, codificándolos de una manera segura para evitar ser atacados por terceros quienes podrían distorsionar el mensaje o peor aún negar el envío del mismo, una vez recibido el mensaje se debe decodificar utilizando la misma función para que sea entendible.

Cabe recalcar que al mantener la integridad se tendrá claro el tiempo en que viaja el mensaje por la Red desde el emisor hacia el receptor sin interrupción alguna.

5.2.3 No repudio

El objetivo de este aspecto es garantizar y demostrar pruebas que podrían presentarse a terceras personas para dar a conocer que una determinada acción ha tenido lugar, de manera que una persona o una entidad no podrán negar haber realizado una operación o un proceso. Viéndolo desde el punto del e-commerce se puede decir que el no repudio de origen protege al receptor de la negación del envió del mensaje por el emisor, por otro lado el no repudio de recepción protege al emisor de que el receptor pueda negar el mensaje recibido, como ejemplo tenemos a las transacciones, las mimas que se ejecutan al momento de hacer una compra, es decir, no se podrá negar dicho movimiento por ninguna de las partes.

Es una forma clara de mantener la seguridad en el negocio virtual, dando la confianza necesaria para que el cliente realice sus compras sin ningún problema, permitiéndole que el pago sea confiable tanto para el usuario como para la entidad bancaria.

5.2.4 Autenticidad

El cliente se maneja por la seguridad que ofrece una tienda virtual, es decir al momento de ingresar a una tienda en línea, es importante requerir de un ingreso con credenciales personales, de manera que los datos del cliente no sean visibles y accesibles para las personas que se encuentren en la red.

Los clientes tienen el temor a la modificación de información y al fraude al momento de comprar en línea, es por eso que los mensajes de seguridad tanto de envío como de recepción son transportados de manera encriptada, para reconocer la identidad de una persona en la web se deberá descencriptar los datos con el mismo

algoritmo para proceder a comparar y se verificar si la información se trata de la persona quien dice ser y pueda proceder con la compra.

A cada cliente se le asigna un usuario y una contraseña, adicional llenan un formulario con datos necesarios para emitir una factura luego de un pedido; al momento de digitalizar la compra se solicitará la identificación primaria del cliente para imprimir la factura con los datos antes grabados. La información del comprador no se mostrará de manera constante; por lo que se podrá brindar confianza a los usuarios respecto a la identidad, los datos de los mismos se quedarán guardados de una manera codificada en la base de datos de la tienda virtual o de la entidad de pago gracias a los denominados "Certificados Digitales".

5.2.5 Responsabilidad

Cada una de las Instituciones tienen sus propias políticas de Seguridad, las mismas que deben ser concretas y específicas, construidas de manera que las partes involucradas en dicha institución queden satisfechas, dichas normas deben ser claras y estar visibles tanto para los que prestan el servicio como para aquellos que lo reciben, de manera que les permiten tomar soluciones y decisiones al momento de presentarse situaciones inadecuadas.

La ISO 25010 define a la responsabilidad como la "*Capacidad de rastrear de forma inequívoca las acciones de una entidad*", y si se hace referencia éste concepto al comercio en línea y más específicamente a las entidades que realizan los servicios de pagos, como son Verified by Visa, SecureCode de MasterCard, PayPal, se puede afirmar que cada una de ellas cuentan con Políticas de Responsabilidad, donde explican claramente las situaciones a los que dicha entidad

se hacen responsables, así como también las excepciones, es decir cuando el portal web o el usuario debe asumir la responsabilidad.

5.2.6 Comparaciones

Seguridad	Confidencialidad	Integridad	No-Repudio	Autenticidad	Responsabilidad
MasterCard	Guarda y mantiene la Información de Activación sin compartir a terceros, con excepción de procesos legales.	Utiliza un protocolo de seguridad SSL, además cuenta con la opción de que los usuarios puedan informar de manera inmediata cualquier uso no autorizado de su contraseña o información de validación, o cualquier problema de seguridad.	Las firmas digitales aseguran que el firmante o el comprador no pueden repudiar su acción.	Se requiere crear Usuario y Contraseña o se asigna un Usuario y Contraseña antes de que se acepte el pago.	El sistema será responsable solo en caso de fraude y de que el tarjetahabiente haya cumplido con las clausulas establecidas en las políticas y los términos de referencia.

Visa	No comparte ningún tipo de información personal salvo el caso de que el usuario lo permita.	Se utiliza el protocolo SSL para páginas Web y el protocolo mobile 3D para asegurar el pago a través de teléfonos móviles.	El servicio de Visa, Verified garantiza el no repudio de las transacciones en red a través de un proceso para confirmar la identidad del tarjetahabiente.	Verifica con el banco la autenticidad de la tarjeta de crédito, además permite utilizar una clave o contraseña (que sólo el tarjetahabiente conoce) para autorizar la compra.	Cuenta con una política denominada "cero responsabilidad", donde el tarjetahabiente quedará libre de responsabilidad en caso de que su tarjeta, la información de la cuenta, o el comercio realicen fraude.
PayPal	No comparte información	Tiene certificado PCI-DSS, los mismos que	El pago mediante PayPal es seguro,	La autenticación se realiza mediante	PayPal tiene cuenta con varias políticas de

	personal ni financiera a los comercios PayPal, al contrario los mantiene almacenados de forma segura en su servidor.	aseguran una integridad de los datos de los clientes, pues cumplieron con el programa de seguridad de la tarjeta Visa y MasterCard; además posee un certificado del Instituto Estadounidense sobre la declaración de estándares de auditoría (SAS70).	evitando su interceptación no autorizada y garantizando el no repudio.	correo electrónico verificado, a lo que se obtiene una respuesta por el mismo método.	seguridad para cancelaciones, protección del comprador, reembolsos, etc. Revisar ANEXO Políticas PayPal.

Tabla 10. Comparación de las características de "Seguridad" según norma ISO 25010 entre Visa, MasterCard y PayPal (Elaboración: Autoras. Cuenca-Ecuador 2014).

5.2.7 Conclusiones Análisis de Seguridad:

Como se explicó, la norma ISO 25010 se encarga de medir la calidad de un producto software con diferentes características, por motivo de tratarse de un análisis de seguridad en el e-commerce, se ha hecho referencia a este eje, el mismo que hace alusión a la capacidad que tienen los mecanismos de pago Verified by Visa, SecureCode de MasterCard y PayPal, para proteger la información personal y financiera de cada uno de los tarjetahabientes, de manera que no puedan ser modificados, ni tener fraude alguno. Esta característica de la ISO 25010 obliga al cumplimento de 5 aspectos: confidencialidad, integridad, no-repudio, autenticidad, responsabilidad; para garantizar que el software cumple con la seguridad necesaria, brindando de esta manera tranquilidad y confianza para que los clientes puedan realizar transacciones en línea.

Luego del análisis realizado a los servicios (Verified, SecureCode, PayPal) de las distintas entidades financieras, se puede afirmar que en la propiedad de:

- Confidencialidad: Sabiendo que ésta hace referencia a la protección de la información personal y financiera de los tarjetahabientes, se puede concluir mencionando que los datos de los clientes se mantienen seguros en cualquiera de las 3 casas financieras, teniendo en cuenta que cada una de ellas tienen sus propias políticas.
- Integridad: Siendo indispensable la información de los clientes es importante que la misma no sufra cambios de terceras personas, esto se lleva a cabo a través de firmas y certificados digitales con los que sí cuentan Visa, MasterCard. PayPal al ser una entidad de pago adicional a los SSL y SET de

Visa y MasterCard cuenta también con una certificación otorgada por el Instituto Estadounidense sobre la declaración de estándares de auditoría (SAS70)

- No-Repudio: Verified, SecureCode, PayPal garantizan el no repudio, es decir que los compradores que se autenticaron con estas organizaciones y realizan una transacción no pueden rechazar dicha acción o viceversa
- Autenticidad: Todas las instituciones financieras tienen uno o varios métodos para poder demostrar la identidad de una persona o empresa, así por ejemplo en Visa y MasterCard el tarjetahabiente cuenta con una clave personal y única con la que podrá realizar transacciones; por otro lado PayPal se maneja de una manera distinta pues la autenticación se realiza mediante un e-mail que son validados y seguros por esta entidad.
- Responsabilidad: Según la Real Academia Española, responsabilidad se define como "*Obligación de reparar y satisfacer, por sí o por otra persona, a consecuencia de un delito, de una culpa o de otra causa legal*"; de esta manera cada una de las casas financieras cuenta con políticas donde se estipulan una o varias normas de responsabilidad, las misas que verifican acciones de los comercios electrónicos con lo que a transacciones se refiere; es decir, si es que el usuario cumple con la normativa establecida y surge un fraude, éste será absuelto de toda responsabilidad.

6 Conclusiones

El crecimiento de las nuevas tecnologías ha marcado grandes cambios en los procesos de compra y venta de bienes y/o servicios, logrando así que las pequeñas y medianas empresas puedan comercializar de manera virtual, y los usuarios adquieran los productos requeridos a través de un dispositivo electrónico y una conexión a Internet, donde podrán elegir artículos, realizar la compra y cancelar mediante el método de pago electrónico.

Una de las grandes ventajas que tiene el cliente al realizar sus compras en línea, es que al momento de utilizar el carrito de compras, el usuario puede agregar diversos artículos, actualizar la cantidad de los mismos; en caso de declinar su compra, el carrito puede ser vaciado o abandonado, permitiendo de ésta manera que el stock no se modifique; por otro lado, el cliente tiene la opción de seguir comprando luego de retornar a la tienda virtual. Cabe recalcar que en el carrito de compras se listan todos los productos seleccionados por el usuario, los mismos que se encuentran detallados y con su respectivo subtotal, que se recalculará al momento de las distintas modificaciones.

Al momento de finalizar la compra el tarjeta-habiente deberá acceder a la página para realizar el pago; ésta cuenta con firmas y certificados digitales, brindando tranquilidad del usuario, ya que para realizar dicho proceso se requiere información confidencial del cliente y de sus tarjetas; los datos son encriptados en distintos algoritmos criptográficos que consisten en aplicar fórmulas matemáticas complejas, volviéndolos de ésta manera ilegibles y garantizando confidencialidad y seguridad.

El pago se lo realiza a través de diferentes entidades bancarias, las mismas que cuentan con políticas propias, funcionamientos y requerimientos ajustados a las necesidades de cada casa financiera como Visa y MasterCard, o con intermediarios como PayPal.

La inversión que se realice a un negocio tradicional para transformarlo en uno virtual, o la iniciación del mismo, será muy rentable, ya que dará un giro de 360 grados a la empresa, pues los clientes al obtener mayores beneficios, incrementarán sus compras, por lo que el comercio contará con mayores ingresos.

Es recomendable que las tiendas virtuales al momento de crear su botón de pagos, para la utilización del carrito de compras, evalúen mediante el Modelo de Calidad ISO 25001 a cada una de las entidades financieras que brindarán sus servicios, pues dicho modelo cuenta con estándares que permiten medir la Seguridad, evaluando de ésta manera diferentes aspectos importantes como la confidencialidad, integridad, no-repudio, autenticidad y responsabilidad.

Una vez conocidos los resultados de una exhaustiva investigación en lo que a análisis costo-beneficio, riesgos, costos, seguridad, y control de calidad se refiere, se pudo constatar que el botón de pago que se realiza en el carrito de compras debería ser arrendado porque los porcentajes en la infraestructura, certificaciones, licencias son muy elevados como para implementar un propio sistema.

Se recomienda que el portal web que cuente con un carrito de compras tenga de preferencia el método de pago PayPal ya que es una institución certificada a nivel mundial que facilita realizar y recibir pagos en línea en distintos lugares e idiomas,

además con cualquier tarjeta de crédito o débito sin compartir información personal o financiera, garantizando de esta forma seguridad, comodidad, y confianza a los usuarios.

7 Referencias

7.1 Apéndice: Glosario

IC: Tarjeta con microprocesador.

PYMES: Pequeña y mediana empresa.

PIN: Número de identificación personal.

CVV: Valor de verificación de la tarjeta.

PCI DSS: Estándar de seguridad de datos para la industria de tarjetas de pago.

ISO: Organización Internacional de estandarización.

SPAM: Mensajes no solicitados, enviados de forma masiva, habitualmente de tipo publicitario.

UML: Lenguaje Unificado de Modelado.

TPB: Dispositivo que sirve para gestionar las tareas de venta al público en un comercio.

CA: Compañía desarrolladora de software.

HASH: Algoritmo matemático.

OTP: Dispositivos generadores de claves de acceso.

KEYLOGGER: Programa que registra y graba la pulsación de teclas.

SCD: Archivos encriptados.

DUKPT: Clave pública, que sirve para descencriptar.

ANSIX 9.52: Modo CBC para el criptoanálisis.

PED: Procesamiento electrónico de datos.

HSM: Dispositivo criptográfico que genera, almacena y protege claves criptográficas.

ISO TR 14742: Estándar de Calidad de criptograma recomendado para servicios financieros.

ISO/IEC 18031: Especifica un modelo conceptual que genera bits randómicamente para propósitos criptográficos.

ISO 9564: Estándar internacional para el manejo y seguridad del PIN.

ISO 11568: Especifica las principales reglas que deben usar las llaves en los criptosistemas.

MITB: Ataque informático orientado al robo de datos bancarios.

ATM: modo de transferencia asíncrona.

SSL: protocolo criptográfico que proporciona transferencia de datos de manera segura.

HTTP: Protocolo de transferencia de hipertextos.

PCI: Security Standards Council es un foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas.

SET: Es un protocolo elaborado por iniciativa de VISA y MasterCard, en donde cada clave pública va asociada a un certificado de autenticidad emitido por una autoridad de certificación (AC).

IRC: Centro de Recursos de Internet.

IIS: Servidor de Información de Internet.

QA: Garantía de Calidad.

7.2 Bibliografía

Algoritmos Criptográficos. 2012. Algoritmo DSA. Enero 2014. http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/5-criptografia-asimetrica-o-de-clave-publica/56-firmas-digitales/562-dsa-digital-signature-algorithm

Algoritmos Criptográficos. 2008. Algoritmo IDEA. Enero 2014. http://iie.fing.edu.uy/ense/asign/dsp/proyectos/1999/cripto/descripcion.html

Algoritmos Criptográficos. 2010. Ejemplo RIJNDAEL. Enero 2014 http://www.formaestudio.com/rijndaelinspector/archivos/rijndaelanimation.html

Algoritmos Criptográficos. 2012. Algoritmo Vigenere. Enero 2014. http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRIPTOGRAFIA/POLIALFABETICAS/cifra%20de%20vigenere.html

Algoritmos Criptográficos. 2013. Criptoanálisis y criptología aplicada. Enero 2014. http://www.docstoc.com/docs/104692743/Algoritmos-criptogr%25EF%25BF%25BDficos

ANETCOM. 2012. Guía práctica de E-commerce para PYMES. Mayo 2014. http://video.anetcom.es/editorial/GUIA_E-COMMERCE_BR.pdf.

CABALLERO, Pino. Seguridad Informática – Técnicas Criptográficas. 1997.

COMPUTERWORLD. 2014. Era Digital. Mayo 2014

Delitos Informáticos. 2012. Seguridad en Comercio Electrónico. Abril 2014. http://delitosinformaticos.com/ecommerce/cargos.shtml.

DELL. 2011. Fundamentos de los Servidores DELL. Mayo 2014. http://www1.la.dell.com/content/topics/segtopic.aspx/es/dell-server-basics-buy-guide?c=mx&l=es&cs=mxbsdt1.

Desarrollo E-commerce. 2013. Consultoría y desarrollo e-commerce. Mayo 2014. www.livecommerce.es.

Diagramación. 2009. Diagrama de Interacción. Noviembre 2013. http://gidis.ing.unlpam.edu.ar.

EBay. 2014. Formas de Pago. Abril 2014. http://pages.ebay.es/help/pay/methods.html#paypal.

EcuRed. 2012. Algoritmo ELGamal. Febrero 2014. http://www.ecured.cu/index.php/ElGamal

Elegir una forma de pago. 2014. EBay. Abril 2014. http://pages.ebay.es/help/pay/methods.html#paypal.

Elegir una forma de pago. 2014. EBay. Abril 2014 https://www.paypal.com/ec/webapps/mpp/paypal-safety-and-security.

Encriptación. 2013. Algoritmos - Encriptación. Diciembre 2013. http://www.alegsa.com.ar/Dic/encriptacion.php.

Escuela Universitaria de Informática de la Universidad Politécnica de Madrid-España. 1999 Seguridad. Abril 2014.

E.S.O. 2011.Encriptación y Esteganografía. Abril 2014. http://www.matematicas.isdata.es/index.php/home/340-encriptacion-y-esteganografia.

FERNANDEZ, Santiago. Criptografía Clásica. Abril 2004. http://www.hezkuntza.ejgv.euskadi.net/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf

FIT for E-commerce. 2010. Seguridad en Comercio Electrónico. Mayo 2014. http://proin.ktu.lt/~virga/leonardo_fit/materials/es/basic_modules/m7/downloads/chapter5.pdf.

Formas de Pago. 2014. PayPal. Abril 2014. http://pages.ebay.es/help/pay/methods.html#paypal.

GOMEZ, Álvaro. Sistemas Criptográficos Simétricos. 2013. Modos Algoritmos Simétricos. Febrero 2014. http://www.7colombia.com/seguridad_informatica/09%20-%20Anexo%20IX%20-%20Sistemas%20criptogr%E1ficos%20sim%E9tricos.pdf

Historia. 2013. PayPal. Abril 2014. https://www.paypal-media.com/es/history.

ISO 25000. 2014. Calidad del Producto software. Mayo 2014. http://iso25000.com/index.php/normas-iso-25000/iso-25010.

KING, Jeremy. Security Standards Council. 2010. Understanding the PTS Security. Abril 2014. https://www.pcisecuritystandards.org/pdfs/webinar_100519pci_pts_3.0.pdf.

Ley de Comercio Electrónico. 2006. Consejo Nacional de Telecomunicaciones. 18 Diciembre 2014.

MasterCard Standard. 2014. MasterCard. Enero 2014. http://www.pacificard.com.ec/mastercard/tipos.aspx.

Ministerio de Telecomunicaciones del Ecuador. 10 de Junio 2014. http://www.telecomunicaciones.gob.ec/

Modos Criptográficos. 2014. Clasificación de Modos. Febrero 2014. http://slideplayer.es/slide/106683/

MUÑOZ, Alfonso. Seguridad Europea. 2004. Rijndael. Enero 2014. http://www.tierradelazaro.com/cripto/AES.pdf

PacifiCard. 2014. Pasos funcionamiento de SecureCode. MasterCard Marzo 2014. http://www.pacificard.com.ec/

PacifiCard. 2014. Tipos de Tarjetas de Crédito. MasterCard Marzo 2014. http://www.pacificard.com.ec/mastercard/tipos/mastercard-black.aspx

PayPal. 2014. Historia. Abril 2014. https://www.paypal-media.com/es/history.

PayPal. 2014. Política de Privacidad. Abril 2014. https://www.paypal.com/ar/webapps/mpp/ua/privacy-full?locale.x=es_AR.

Paypal. 2014. Safety and Security. Mayo 2014. https://www.paypal.com/es/webapps/mpp/paypal-safety-and-security

Paypal. 2014. Tarifas Paypal. Mayo 2014. https://www.paypal.com/ar/webapps/mpp/ua/privacy-full?locale.x=es_AR

PCI DSS. 2014. Payment Card Industry Data Security Standards. Abril 2014. http://www.sia.es/images/06-Folleto%20Comercial%20-%20Servicios%20PCI-DSS_v2.1.pdf.

PCI Security Standard s Council LLC. 2013. Payment Card Industry. Marzo 2014. https://www.pcisecuritystandards.org/documents/PCI_PED_General_FAQs.pdf

PERALTA, Luis. Secure Net. 2002. Algoritmos Asimétricos. Marzo 2014 http://www.udb.edu.sv/udb/archivo/guia/electronica-ingenieria/seguridad-en-redes/2013/i/guia-4.pdf

PINTADO, Pablo. Criptografía Simétrica. Universidad del Azuay. 2012

Plan de Marketing. 2003. Estrategias de Mercado. Octubre 2013. http://www.guia.ceei.es/interior.asp?MP=8&MS=7.

Protección al comprador de PayPal https://www.paypal.com/ec/webapps/mpp/security/sell-chargebackguide1

Protocolos de Comunicación. 2010. RSA. Febrero 2014. http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/rsa.html

Protocolos de Seguridad. 2012. SSL. Febrero 2014.

http://www.4d.com/4d_docstatic/4D/12.4/Utilizar-el-protocolo-SSL.300-977193.es.html

Protocolos de Seguridad. 2014. SSL. Febrero 2014.

http://www.expresionbinaria.com/certificados-de-seguridad-ssl-funcionamiento-tipos-y-caracteristicas/

Robert D. Austin. Harvard Business Review, 2003.

SARMIENTO, Manuel. Responsabilidad Civil. Universidad de Colombia. 2002.

SEBASTIAN Bortnik, Gerente de Educación & Servicios de ESET Latinoamérica. 2012.

Seguridad Informática. 2013. PCI DSS, PA DSS, PCI PTS. http://seguinfo.wordpress.com/2013/01/03/normas-de-seguridad-pci-dss-pa-dss-y-pci-pts/.

Seguridad y Encriptación de Datos. 2010. Algoritmo DES. Enero 2014. http://pitagoras.usach.cl

SERVERS. 2014. Tecnología RAID servidor. Junio 2014. http://www.informaticamoderna.com/Servidor.htm.

Superintendencia de Bancos y Seguros. 2011. Riesgos. Marzo 2014. http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_IX_cap_II-1.pdf

Symantec. 2014. Certificados SSL. Mayo 2014. http://www.verisign.es/.

TECNOAVAN. 2007. Tecnologías y Arquitecturas. Mayo 2014. http://www.comercioelectronico.tecnoavan.com/elementos.html.

Términos de Uso. 2011. MasterCard. Febrero 2014. https://www.bncr.fi.cr/BNCR/BNSecure/PDF/BNCR%20-%20BN%20Secure%20-%20Terminos%20y%20condiciones%20MCSC.pdf

Tipos de criptografía. 2011. Simétrica, Asimétrica. Enero 2014. http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Transacciones PayPal.2013.PayPal. Abril 2014. http://es.meet-magento.com/paypal.

Tutorial UML. 2000.___ Business Process Modeling. Noviembre 2013. www.sparxsystems.com.au/UML_Tutorial.htm

Unified Modeling Language. 2014. Introduction to UML. Noviembre 2013. www.uml.org

Universidad Pontificia Comillas ICAI, Madrid 2006 El Arte de Resguardar Información. Abril 2014.

Ventajas Verified by Visa. 2014. Visa Europe. 3 mayo 2014. http://www.visaeurope.es/su-tarjeta-visa/compre-en-internet-verified-by-visa/ventajas

Visa. 2002. Visa PIN Security Requirements Auditor's Guide. Diciembre 2013

Visa. 2014. Políticas de Privacidad. Marzo 2014. http://lac.visa.com/about/privacy.jsp.

Web design and development. 2014. Soluciones para tu e-commerce. Mayo 2014. http://www.ma-no.org/es/content/index_las-10-mejores-soluciones-para-tu-e-commerce_1833.php