ANÁLISIS DE LA SEGURIDAD INFORMÁTICA EN LAS TRANSACCIONES ELECTRÓNICAS PARA EL COMERCIO ELECTRÓNICO

CRISTIAN CAMILO SABOGAL BELTRÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
PROGRAMA: PROYECTO DE GRADO
BOGOTÁ
2021

Análisis de la seguridad informática en las transacciones electrónicas para el comercio electrónico

Cristian Camilo Sabogal Beltrán

Monografía presentada para optar al título de: Especialista en seguridad Informática

Director:
Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia
Especialización en seguridad Informática
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

DEDICATORIA

Dedico esta tesis a mi mamá Teresa, a mis hermanas Viviana y Andrea y a mi novia Alejandra.
A todos aquellos docentes y tutores que me acompañaron en todo este proceso y me guiaron a partir de su conocimiento.
Y a todos aquellos que de alguna u otra manera hicieron parte de este proceso de mi vida académica.

Camilo, 2021

AGRADECIMIENTOS

Agradezco a Dios, por guiarme y cuidarme en cada paso de mi vida.

A mi madre, mis hermanas y mi novia por el amor y la paciencia que me dieron durante todo este proceso académico, por estar conmigo en mis logros y en cada momento de mi vida.

A mis tutores y docentes, que guiaron cada paso de este proyecto con su conocimiento y consejos académicos.

Y en general a todos los que de una u otra forma contribuyeron a este logro porque con sus consejos y aciertos, contribuyeron y fortalecieron mi conocimiento.

Camilo, 2021

ÍNDICE GENERAL

LISTA DE IMÁGENES

LISTA DE TABLAS

GLOSARIO

1. **Amenazas cibernéticas:**

   Son intentos de interrumpir o infiltrarse en un sistema o una red de computadores.[1]

2. **Análisis de seguridad:**

   Un análisis de seguridad es un enfoque de la seguridad digital que analiza datos con el único objetivo de detectar anomalías o un comportamiento inusual de usuarios y otras amenazas que puedan existir. La inteligencia artificial y aprendizaje automático ayudan a automatizar el proceso de detección y solución. [2]

3. **Estándares de seguridad**:

   Es un conjunto de normas que contienen dentro de sí buenas prácticas para el establecimiento, mantenimiento y mejoras de Sistemas de Gestión el Seguridad de la Información.[3]

4. **Pago electrónico:**

   Son un sistema de pago que facilita la aceptación de pagos para la realización de transacciones sin tener que usar dinero en efectivo, el gran avance de las tecnologías de la información dentro de sistemas financieros

---

[1] WELLS FARGO. Estafas y amenazas cibernéticas. [Sitio WEB]. Miami. Zelle. [marzo, 2020]. Disponible en https://www.wellsfargo.com/es/privacy-security/fraud/bank-scams/

[2] CITRIX. [Sitio WEB]. México. Análisis de seguridad. [marzo, 2019]. Disponible en https://www.citrix.com/es-mx/solutions/analytics/what-is-security-analytics.html

[3] GOBIERNO DE ESPAÑA. Normas ISO sobre gestión de seguridad en la información. [Sitio WEB]. Madrid. Aula Mentor. [diciembre 2019]. Disponible en http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

ha permitido el surgimiento de estos nuevos medios de pago que cada día se usan más a nivel mundial. [4]

5. Pagos en línea PSE:

Es un sistema centralizado y estandarizado, que fue desarrollado en un principio desarrollado por ACH Colombia, mediante el cual las diferentes empresas brindan a los usuarios la posibilidad de desarrollar pagos y/o compras a través de internet, debitando recursos en la entidad financiera donde estos tengan su dinero y depositándolo en las cuentas de las empresas. [5]

6. Seguridad en la información:

Es un conjunto de técnicas y medidas para controlar los datos que se manejan dentro de una organización para asegurar que esta información no salga del sistema que ha sido implementado por la empresa. están basadas en nuevas tecnologías pues resguarda la información a la que solo tienen derecho ciertas personas que han sido previamente autorizadas. Debe ser crítica, valiosa y sensible. [6]

7. Vulnerabilidades:

Una vulnerabilidad es un fallo o una debilidad en el sistema de la información que pone en riesgo la seguridad de esta, de esta forma se permite que un

---

[4] BANCO DE CRÉDITO. Educación financiera. [Sitio WEB]. Bogotá. [enero, 2020]. Disponible en https://www.bancoprocredit.com.co/images/docs/5_Educacion_Financiera/Medios-de-pago-electronico.pdf

[5] UNIVERSIDAD CATOLICA. Facultad de ingeniería, seguridad en la web. [Sitio WEB]. Bogotá. [abril, 2019]. Disponible en https://portalweb.ucatolica.edu.co/paw/index.php?option=com_content&view=article&id=8&Itemid=29

[6] OBS BUSINESS SCHOOL. Seguridad de la información, un conocimiento imprescindible. [Sitio WEB]. Lima. Planeta formación y universidades. [9 de octubre 2017]. Disponible en https://obsbusiness.school/es/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible

atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la información. [7]

[7] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Amenaza vs vulnerabilidad. [Sitio WEB]. Madrid. Ens. [marzo, 2017]. Disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

SUMMARY

1. Cyber Threats:

Are attempts to interrupt or infiltrate a system or a computer network.[8]

2. Security analysis:

A security analysis is a digital security approach that analyzes data with the sole objective of detecting anomalies or unusual user behavior and other threats that may exist. Artificial intelligence and machine learning help automate the detection and resolution process.[9]

3. Security standards:

It is a set of norms that contain within themselves good practices for the establishment, maintenance and improvement of Information Security Management Systems.[10]

4. Electronic payment:

They are a payment system that facilitates the acceptance of payments to carry out transactions without having to use cash, the great advancement of

[8] WELLS FARGO. Estafas y amenazas cibernéticas. [Sitio WEB]. Miami. Zelle. [marzo, 2020]. Disponible en https://www.wellsfargo.com/es/privacy-security/fraud/bank-scams/

[9] CITRIX. [Sitio WEB]. México. Análisis de seguridad. [marzo, 2019]. Disponible en https://www.citrix.com/es-mx/solutions/analytics/what-is-security-analytics.html

[10] GOBIERNO DE ESPAÑA. Normas ISO sobre gestión de seguridad en la información. [Sitio WEB]. Madrid. Aula Mentor. [diciembre 2019]. Disponible en http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

information technologies within financial systems has allowed the emergence of these new means of payment that every day is used more worldwide.[11]

5. Online PSE payments:

It is a centralized and standardized system, which was originally developed by ACH Colombia, through which the different companies provide users with the possibility of developing payments and / or purchases through the internet, debiting resources in the financial entity where they have their money and depositing it in the accounts of the companies.[12]

6. Information security:

It is a set of techniques and measures to control the data that is handled within an organization to ensure that this information does not leave the system that has been implemented by the company. They are based on new technologies because it safeguards the information to which only certain people who have been previously authorized are entitled. It must be critical, valuable and sensitive.[13]

7. Vulnerabilities:

A vulnerability is a flaw or weakness in the information system that puts its security at risk, thus allowing an attacker to compromise the integrity, availability or confidentiality of the information.[14]

---

[11] BANCO DE CRÉDITO. Educación financiera. [Sitio WEB]. Bogotá. [enero, 2020]. Disponible en https://www.bancoprocredit.com.co/images/docs/5_Educacion_Financiera/Medios-de-pago-electronico.pdf

[12] UNIVERSIDAD CATOLICA. Facultad de ingeniería, seguridad en la web. [Sitio WEB]. Bogotá. [abril, 2019]. Disponible en https://portalweb.ucatolica.edu.co/paw/index.php?option=com_content&view=article&id=8&Itemid=29

[13] OBS BUSINESS SCHOOL. Seguridad de la información, un conocimiento imprescindible. [Sitio WEB]. Lima. Planeta formación y universidades. [9 de octubre 2017]. Disponible en https://obsbusiness.school/es/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible

[14] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Amenaza vs vulnerabilidad. [Sitio WEB]. Madrid. Ens. [marzo, 2017]. Disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

RESUMEN

El comercio electrónico o e-commerce, no es otra cosa sino la compra y venta de productos o servicios a través de medios electrónicos como internet u otras redes informáticas. Aproximadamente en los años 70, hicieron su primera aparición algunas relaciones comerciales que utilizaban un computador para transmitir datos, como por ejemplo órdenes de compra o facturas.

El comercio electrónico se perfila para ser en un futuro la razón de ser del comercio y de los negocios, no solo está enfocado a grandes empresas y/o multinacionales, pues son muchas las medianas y pequeñas empresas que ofrecen sus productos y servicios a través de una plataforma electrónica, por lo anterior el uso efectivo y seguro de la información, es la base fundamental para lograr negocios competitivos que se desarrollen, a gran escala en la web.

La seguridad informática, consiste en asegurar los recursos de información de determinada organización, y garantiza que esta solo pueda ser modificada o manipulada por personas que la empresa autorizó previamente.

Por lo anterior, los protocolos de seguridad son indispensables, y definen las reglas que gobiernan las telecomunicaciones y están diseñadas para que el sistema en el cual es aplicado pueda soportar ataques de carácter malicioso. El SSL es el protocolo más seguro que existe y es el más usado a nivel mundial; funciona como un túnel que protege toda la información que se envía y se recibe.

En conclusión, la presente monografía, tiene como finalidad analizar cada uno de los protocolos y/o mecanismos que algunas empresas han aplicado para garantizar la seguridad en las transacciones electrónicas para el comercio electrónico.

ABSTRACT

Electronic commerce or electronic commerce is nothing else but the purchase and sale of products or services through electronic means such as the internet or other computer networks. Approximately in the 70s, some commercial relationships that used a computer to transmit data, such as purchase orders or invoices, made their first appearance.

Electronic commerce is shaping up to be in the future the raison d'être of commerce and business, it is not only focused on large companies and / or multinationals, as there are many medium and small companies that offer their products and services through an electronic platform, therefore the effective and safe use of information, is the fundamental basis to achieve competitive businesses that develop, a large scale on the web.

Computer security consists of guaranteeing the information resources of a certain organization and guarantees that it can only be modified or manipulated by people that the company previously authorized.

Therefore, security protocols are essential, and modify the rules that govern telecommunications and are determined so that the system in which it is applied, can control attacks of a malicious nature. SSL is the most secure protocol that exists and is the most widely used worldwide; It works like a tunnel that protects all the information that is sent and received.

In conclusion, the present monograph has the application of analyzing each of the protocols and / or mechanisms that some companies have applied for security in electronic transactions for electronic commerce.

INTRODUCCIÓN

La presente monografía, hace referencia a la gestión y análisis de los diferentes mecanismos existentes en cuanto a la seguridad de transacciones electrónicas se refiere, con el fin de demostrar la gran importancia que estos tienen y por qué deben ser implementados dentro de una organización prestadora de servicios que ofrezca a sus usuarios y/o clientes la opción de pagar y comprar por medio de plataformas electrónicas, generando del mismo modo una sensibilización tanto en empresas como en usuarios a la hora de ofrecer y hacer uso de estas plataformas.

Se define seguridad informática como un proceso de prevención y detección del uso no adecuado y no autorizado de un sistema informático determinado. Además, implica el proceso de proteger los recursos informáticos y la información consignada allí de intrusos con intenciones maliciosas. La seguridad informática debe cumplir 4 pautas generales; debe ser confidencial, es decir que solos los usuarios autorizados pueden acceder a la información, datos o recursos; integra, pues solo los usuarios autorizados tienen la capacidad de modificar los datos cada vez que sea estrictamente necesario; por otro lado debe ser disponible, es decir que los datos allí almacenados siempre deben estar disponibles cuando el usuario autorizado lo requiera; por último, la seguridad informática debe ser autentica, debe dar la seguridad de que el usuario está manteniendo comunicación con quien este cree.

En cuanto a la seguridad en las transacciones online, hay 6 aspectos que una organización debe contemplar cuando decida implementar el pago o compra de servicios y/o artículos por la web; verificación de la identidad del cliente, seguridad en las transacciones web, seguridad del sitio web, privacidad, utilidad de la criptografía y autenticación del sitio web desde el punto de vista del usuario, lo anterior con el fin de asegurar que la transacción es segura y confiable para el cliente.

Por lo anterior, la idea de este documento, es analizar y gestionar los diferentes mecanismos y/o estrategias que ya han sido implementadas en diferentes organizaciones, con el fin de ofrecer a sus usuarios total seguridad a la hora de adquirir sus productos o servicios por medio de una plataforma electrónica; del mismo modo, desde el aspecto legal, busca revisar algunas de las leyes que diferentes países, especialmente Colombia han implementado con el fin de castigar a quienes cometen delitos informáticos.

1. DEFINICIÓN DEL PROBLEMA

El proyecto en mención basa su accionar en analizar y gestionar cada uno de los mecanismos y estrategias que diferentes empresas han implementado con el fin de proporcionar seguridad a cada uno de los tarjeta habientes que se han convertido en sus clientes, a través del uso de plataformas electrónicas para hacer pagos y comprar determinados artículos.

El uso de los diferentes medios de pago que involucran plataformas electrónicas genera algunas desventajas, los pagos móviles, algunas veces presentan fallos en su seguridad, pues hay plataformas que aún no son 100% seguras, además de ello, las plataformas utilizadas por determinada empresa y/o organización puede ser vulnerable frente a los ataques de personas maliciosas o algún virus que pueda alterar o robar la información que los usuarios o clientes ingresan.
Algunas de las desventajas que presenta el E-Commerce, son las siguientes:

- La competencia es mayor pues cualquier persona puede poner en marcha este tipo de productos.
- Existen consumidores que no comprar el articulo hasta no verlo, desconfían de los pagos en línea.
- No todos los productos se pueden vender en línea con la misma facilidad.
- Los gastos de envío pueden resultar muy elevados.
- Fidelizar un cliente es demasiado complejo por la gran cantidad de competencia que existe.
- Se corre el riesgo de sufrir robos de clave y contraseñas o algún otro acto malintencionado.

Con lo anterior se evidencia que uno de los riesgos que representa el E-Commerce a sus usuarios es el posible robo de claves y contraseñas y de este modo la alteración de datos y el robo de dinero; es aquí donde se identifica el problema y fundamento la presente monografía, pues los riesgos en las diversas plataformas están latentes todo el tiempo y por ello las empresas y organizaciones se han visto obligadas a diseñar e implementar mecanismos y estrategias dispuestas a combatir los delitos informáticos y que aumenten el nivel de seguridad en las operaciones de pago y compra que sus usuarios llevan a cabo; entonces se busca analizar y gestionar algunos de estos mecanismos con el fin de evaluar cómo actúan en pro de la seguridad en las transacciones electrónicas.

1.1. ANTECEDENTES

El comercio electrónico es un tema que ha tenido gran auge en los últimos tiempos, 8 de cada 10 empresas están o han incursionado en el tema de las ventas por internet y 9 de cada 10 personas prefiere usar la web para hacer pagos y compras de determinados bienes o servicios; así mismo la seguridad en la información es un tema que ocupa muchas páginas y que llama mucho la atención, pues una página de ventas en la web es exitosa en gran parte si ofrece a sus clientes y/o usuarios seguridad a la hora de hacer pagos o de incluir datos personales o datos sensibles. Por lo anterior, se han desarrollado algunos proyectos que han tratado tal tema y lo han desarrollado enfáticamente, para la elaboración de este documento investigativo se toman como referencia dos de estos, una tesis de la universidad Javeriana, sustentada y aprobada y cuyo tema central es la seguridad en el comercio electrónico, por otro lado, un repositorio presentado por Fredy Acevedo Zamorano en la Universidad de Chile, para la Facultad de ciencias económicas, que basa su argumento en la seguridad dentro del comercio electrónico y en las ventajas y desventajas que genera el uso del e-commerce.

Héctor José García Santiago, en su tesis de grado, presentada a la Universidad Javeriana; aborda temas acerca de la seguridad en el comercio electrónico, marco jurídico y normas que regulan y sancionan, así como los riesgos a los que una persona se enfrenta a la hora de navegar en una página o sitio web[15]; dentro de los puntos más importantes del documento se resalta la importancia que da a la seguridad dentro de todo lo que significa el comercio electrónico, él indica que no existe e-commerce viable sin seguridad optima y basa sus argumentos en una encuesta publicada por CNN En Español donde los resultados arrojaron que el 91% de las personas encuestadas asegura que sienten que el internet actualmente es demasiado inseguro al momento de comprar artículos o adquirir servicios. Héctor soporta muchos de sus argumentos en encuestas, algunas ya realizadas por empresas y canales de televisión y otras realizadas por el mismo durante el proceso de investigación y realización del documento.

Por otro lado, Fredy Acevedo Zamorano dentro del repositorio que presenta ante la Facultad de ciencias económicas de la Universidad de Chile, argumenta que una de las preocupaciones más grandes de las personas que deciden usar el comercio electrónico es la privacidad de sus datos, como el número y clave de su tarjeta de crédito, direcciones entre otros datos sensibles del usuario, e indica que es una

[15] GARCIA SANTIAGO, Héctor José. Bogotá: Tesis, facultad de derecho, Universidad Javeriana, 2018. P.40

tarea pendiente y ardua por parte de los gobiernos y de los comercios brindar seguridad y confianza a los miles de internautas que hay alrededor del mundo actualmente[16].

Dentro de las ventajas del e-commerce menciona:

- Negociar con clientes
- Negociar con proveedores
- Relación online
- Servicio pre y post venta
- Reducción de costos
- Prolongación del negocio
- Personalización del trato
- Formas de pago más agiles

Argumenta que dentro de las ventajas mencionadas la que más atrae a los usuarios es que el comercio electrónico ofrece variadas formas de pago, pero indica que, si bien esto es atrayente, estos modos de pago no ofrecen total seguridad y confiabilidad en la información.

Como se puede evidenciar los dos proyectos expuestos brevemente presentan temáticas similares a las que el lector podrá encontrar en este documento, anteponiendo la seguridad en la información como eje principal de desarrollo de la temática y abordando el tema del comercio electrónico de manera completa y minuciosa.

1.2. PLANTEAMIENTO DEL PROBLEMA

Como ya se ha expuesto antes, el comercio electrónico ha crecido rápidamente y ha tomado mucha fuerza en el mundo moderno, ha revolucionado la forma en la que interactúan los usuarios con las tiendas o comercios que les interesa, han cambiado la manera de adquirir bienes o servicios, ahorrando tiempo y mejorando su calidad de vida.

Del mismo modo, se ha hecho necesario implementar mecanismos que blinden las múltiples transacciones que a diario se hacen por internet, asegurando los datos que los tarjeta habientes suministran a determinadas páginas, claves, datos

[16] ZAMORANO ACEVEDO, Freddy. Chile: Seminario para optar al título de Ingeniero en formación.

personales entre otra información sensible.

Por lo anterior, y teniendo en cuenta el campo laboral en el que se desenvuelve el autor de este documento y la actividad económica que desarrolla la empresa para que trabaja, se toma la decisión de tratar este tema, pues se ha evidenciado la importancia que tiene la seguridad informática en las diferentes transacciones electrónicas que existen actualmente dentro del desarrollo y uso del comercio electrónico. Son muchos los comercios que actualmente y en pro de hacer crecer sus negocios y de aumentar sus finanzas, deciden incursionar dentro del comercio electrónico, y por ello es vital que estas empresas ofrezcan a sus clientes y usuarios experiencias seguras y confiables al momento en el que estos decidan adquirir los bienes y servicios que ofrecen.

1.3. FORMULACIÓN DEL PROBLEMA

¿De qué manera el análisis sobre la seguridad informática en las transacciones electrónicas, puede contribuir para mejorar la seguridad del sistema digital en el comercio electrónico?

2. JUSTIFICACIÓN

La seguridad de la información, se define como todas aquellas medidas preventivas y de reacción de un individuo u organización para proteger la información, de tal manera, que se asegure la confidencialidad, la autenticidad e integridad de la misma. [17]

Sin embargo, hay que tener en cuenta que la seguridad de la información y seguridad Informática son diferentes; la última, solamente trata la seguridad en los medios netamente informáticos mientras que la primera es para todo tipo de información, ya sea digital o impresa.

La información almacenada es las diversas plataformas electrónicas que existen está siempre expuesta a múltiples riesgos, por ello, las organizaciones e instituciones deben velar siempre por minimizar los riesgos y garantizar la confidencialidad e integridad de los datos; dentro de una organización, existen diversos tipos de información:

Crítica: Es indispensable para la operación y actividad de la empresa.
Valiosa: Es un activo de la empresa, lo que la hace valiosa.
Sensitiva: Debe ser conocida y manipulada únicamente por las personas autorizadas.

Diversas empresas y organizaciones como gobiernos, entidades militares, instituciones financieras, hospitales, empresas privadas entre otras, acumulan una gran cantidad de datos e información confidencial sobre sus clientes, productos ofrecidos y su situación financiera; mucha de esta información es recolectada, tratada y gestionada con el visto bueno de sus usuarios, que luego será trasmitida a través de redes entre máquinas; muchas veces, esta información cae en manos de delincuentes que alteran, modifican y roban parte o la totalidad de la información que fue registrada, lo que genera pérdida de credibilidad entre los clientes pérdida de negocios, demandas legales o en el peor de los escenarios la quiebra total de la empresa.

[17] SOLUCIONES INFORMATICAS TECON. La seguridad en la información. [Sitio WEB]. Alicante. [7 de junio de 2020]. Disponible en https://www.tecon.es/la-seguridad-de-la-informacion/

Por lo anterior, proteger la información se hace muy importante, se vuelve un requisito del negocio, una obligación ética y legal; mientras que, para el individuo, significa respeto a su privacidad y sensación de seguridad a la hora de confiar sus datos más sensibles a determinada empresa.

Ahora bien, del mismo modo en el que la seguridad en la información se hace tan importante en una empresa u organización, la seguridad en el comercio electrónico también juega un papel fundamental, esto teniendo en cuenta que hoy en día más del 60% de las compras se hacen por medio de plataformas electrónicas, según informa la CCCE[18].

Para garantizar la seguridad en las transacciones comerciales, es necesario disponer de un servidor seguro a través del cual toda la información consignada es cifrada y viaja de forma segura, lo que genera confianza tanto en el proveedor como en los compradores que han hecho del comercio electrónico un hábito; al igual que en el comercio tradicional, en el electrónico existe un riesgo, pues hay temor por parte del usuario al realizar una compra por internet, teme por sus datos personales (nombres, número de identificación, número y clave de tarjetas de crédito, direcciones entre otros), de este mismo modo, el proveedor necesita asegurarse de que los datos enviados por el comprador si corresponden a quien está efectuando la transacción.

En consecuencia, se han desarrollado diversos sistemas de seguridad para las transacciones realizadas por internet: Cifrado, Firma Digital y Certificado de Calidad son algunos de los mecanismos que garantizan la confidencialidad, integridad y autenticidad de la información, veremos cada uno detalladamente más adelante.

Por lo anterior, surge la idea de analizar cada uno de los mecanismos, validar su manera de actuar, su importancia, que elementos involucra o necesita para su funcionamiento y que tan vital se hace dentro de la operación de determinada empresa, contemplando las ventajas y desventajas que cada uno de estos mecanismos pueda suponer.

[18] CAMARA DE COMERCIO ELECTRONICA. Ventas por medio de plataformas electrónicas. [Sitio WEB]. Bogotá D.C. [7 de junio de 2020]. Disponible en: https://www.ccce.org.co/noticias/

3. OBJETIVOS

3.1. Objetivo general

Analizar los diferentes mecanismos y/o estrategias de seguridad en las transacciones electrónicas, que diversas empresas han aplicado para asegurar la efectividad en sus transacciones de comercio electrónico.

3.2. Objetivos específicos

- ✓ Identificar los diversos mecanismos y estrategias para la seguridad en las transacciones electrónicas que existen.

- ✓ Determinar cómo actúan y de qué manera se desarrollan los diversos sistemas de seguridad para transacciones comercio electrónico.

- ✓ Establecer y analizar la importancia que tienen los sistemas de seguridad en el comercio electrónico supone para la operación y desarrollo de una empresa y/o organización.

4. MARCOS DE REFERENCIA

4.1. MARCO TEÓRICO

El comercio electrónico, consiste en la compra, venta, distribución, mercadeo y suministro de información de productos y servicios ofrecidos a través de internet. Una de las grandes ventajas que tiene el comercio electrónico es el hecho de que cualquier persona puede acceder a determinado objeto o servicio en cualquier lugar y cualquier momento, lo que genera a los comercios un aumento en sus ventas e ingresos, razón por la cual implementar la opción de comercio electrónico en cualquier negocio es una idea brillante.

A finales de la década de los años noventa y con el desarrollo de las tecnologías informáticas y la gran expansión de las telecomunicaciones, se fortaleció y creció un proceso de globalización e independencia económica que desencadenó en el nacimiento de una forma novedosa e innovadora de realizar actividades comerciales y de esta forma, se creó un nuevo proceso de oferta y demanda, donde tanto clientes como proveedores situaron sus procesos comerciales a través de diferentes medios electrónicos, principalmente por medio de internet; de este modo surgieron empresas y consumidores digitales, cuyas actividades principales dieron vida a lo que hoy conocemos como comercio electrónico o e-commerce.

El e-commerce surge por la necesidad de cubrir la demanda de los negocios globales, pues era necesario la optimización del tiempo y darles un nuevo y mejor uso a las tecnologías; lo anterior, en función de hacer que las empresas sean más competitivas y se dé un valor agregado mediante los pagos electrónicos. [19]

La cámara colombiana de comercio electrónico, mediante un estudio, dio a conocer que el 80% de las personas que navegan en internet en Colombia, consultan o comparan los productos que desean adquirir, el 19% compra y paga en línea y el 17% prefiere comprar en línea, pero pagar una vez reciban el producto en sus casas. [20]

[19] FLOREZ ZABALA, Ana María, Modelo de e-commerce para la implementación de las empresas colombianas. [En línea]. Monografía. ESUMER Institución Universitaria. Medellín. 2019. [07.06.2021]. Disponible en: http://repositorio.esumer.edu.co/bitstream/esumer/2067/1/Modelo%20de%20e-Commerce.pdf

[20] CAMARA COLOMBIANA DE COMERCIO ELECTRÓNICO. [Sitio WEB]. Bogotá: CCCE Estudios y análisis económicos, [07.06.2021]. Disponible en: https://www.ccce.org.co/gestion-gremial/

La Organización Mundial del Comercio, define el e-commerce como, “La producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos”.[21]

Para la construcción de este marco teórico, tomamos como referencia documentos, tesis, repositorios que han sido creados y sustentados alrededor del análisis del comercio electrónico y su seguridad. El primero de ellos, la tesis presentada por Mayra Gabriela Cordero, de la Universidad Católica de Santiago en Guayaquil; dicho documento, indica que algunas de las principales características del comercio electrónico son[22]:

- **Medio de comercio electrónico de trascendencia económica:**

  Es una nueva forma de hacer comercio, va totalmente ajustada a la economía moderna, que se caracteriza por los intercambios, las diferentes exigencias de los clientes y las capacidades que tienen los productores. El comercio electrónico provoca cambios en el contacto entre empresas, clientes, trabajadores por lo que indudablemente va a revolucionar la economía y la eficiencia en la prestación de servicios.

- **Medio de comercio virtual:**

  Los sujetos que intervienen en el comercio electrónico la mayoría de veces no logran conocerse para entablar relaciones inmediatas, pues se encuentran en ciudades o países diferentes.

- **Medio de comercio de bajos costos:**

  El comercio electrónico permite reducir costos de transacción y administración, de este modo también se reducen costos de distribución.

[21] ORGANIZACIÓN MUNDIAL DEL COMERCIO. [Sitio WEB]. México: OMC, Estudios y análisis económicos, [07.06.2021]. Disponible en: https://www.wto.org/spanish/news_s/news20_s/rese_04may20_s.htm

[22] CORDERO LINZAN, Mayra Gabriela. El comercio electrónico e-commerce, análisis actual desde la perspectiva del consumidor en la ciudad de Guayaquil. [En línea]. Monografía. Universidad Católica de Santiago en Guayaquil. Guayaquil. 2019. [07.06.2021]. Disponible en: http://repositorio.ucsg.edu.ec/bitstream/3317/14064/1/T-UCSG-POS-MFEE-179.pdf

Entonces, se clasifica el comercio electrónico en 3 tipos:

- **Comercio electrónico B2B:** esta categoría es conformada por las transacciones de comercio digital de negocio a negocio. Una de las grandes ventajas es que se reduce el costo de la transacción.
- **Comercio electrónico B2C:** la conforman los intercambios comerciales entre empresas y consumidores. Los oferentes a través de una tienda digital ofrecen sus productos a potenciales clientes que visitan la web.
- **Comercio electrónico social:** basa su accionar en el uso de las redes sociales, toda persona que desee vender algo puede publicarlo en su perfil o en perfiles dedicados exclusivamente a la venta y compra de artículos de cierta categoría, así mismo el que desee comprar cierto articulo puede hacerlo a través de las redes.

Los principales medios de pago que ofrece el comercio electrónico son:

- **Pagos con códigos QR:** hace posible realizar formas de forma fácil y segura, solamente basta con pasar el lector sobre el código QR, ingresar la información de la tarjeta en la APP (en caso de que sea la primera vez) y aprobar tanto el monto como el producto o servicio que se está comprando. Hay infinidad de operaciones que se pueden hacer con este medio de pago, abastecer de combustible el auto, comprar sin hacer filas etcétera.
- **Gestión de pagos en Apps:** actualmente tanto las grandes, como medianas y pequeñas empresas cuentan con aplicaciones con medios de pago, como pasarelas, botones que buscan generar una experiencia fácil y confiable al cliente y al proveedor.
- Además de las anteriores, se ha creado una diversa y grande oferta de alternativas de monedas digitales que también permiten al usuario acceder a artículos y servicios ofrecidos por determinadas empresas. El dinero pasó de ser físico a estar en el teléfono móvil.

Ahora bien, en Colombia, el e-commerce ha tenido un gran auge durante los últimos años; en nuestro país 8 de cada 10 colombianos aseguran navegar en internet todos los días, ya sea en sus dispositivos móviles, en su hogar o desde sus lugares de trabajar; el 69% de la población colombiana tiene acceso a internet. [23]

[23] MEZA, Cesar. Experto en marketing digital. Situación actual del uso de internet en Colombia. [Sitio web]. Bogotá. [16.06.2021]. Disponible en: https://cesarmesa.com.co/situacion-actual-del-uso-de-internet-y-redes-sociales-en-colombia/#:~:text=El%2069%25%20de%20la%20poblaci%C3%B3n,4%20horas%20y%2049%20minutos.

Sin embargo, uno de los desafíos más grandes que deben enfrentar las empresas que deciden incursionar en el comercio electrónico es la confianza, pues la mayoría de los clientes y más cuando lo hacen por primera vez, se inquietan por varios temas como por ejemplo la autenticidad del producto y la forma de pago, pues temen que pueda existir algún tipo de fraude, por ello se vuelve fundamental que las plataformas que establecen los comercios cumplan con determinados estándares de seguridad electrónica y ofrecer gran variedad de métodos de pago.

Pese a que se han establecido varios mecanismos de seguridad para blindar el comercio electrónico, en países como Chile y Colombia, se ha masificado el uso de curiosos métodos que han aumentado la inseguridad a la hora de usar este tipo de herramientas. El problema básicamente se ha centrado en el hurto tanto de información financiera como de información personal.[24]

Dentro del comercio electrónico, se habla de cuatro aspectos básicos de seguridad para preservar y blindar los datos de los usuarios y /o clientes de determinada empresa.

- **Autentificación:**

Es el proceso mediante el cual se verifica formalmente la identidad de las entidades que participan en una comunicación o que intercambian información; se entiende por entidad, las personas, procesos o máquinas.

Existen varias formas de autenticación: basadas en claves, basadas en direcciones y criptografía.

De las tres formas mencionadas anteriormente, la más segura es la criptografía, pues tanto en claves como en direcciones hay un riesgo de suplantación de información e identidades.

También se puede hablar de autentificación desde la biometría ya sea de huellas digitales como de la retina del ojo, la voz etcétera, por medio de passwords o por último por medio de un certificado digital que posea el usuario.

[24] AVILES ESPINOZA, Daniela Alejandra. Modelo de adopción de tecnología desde la perspectiva del cliente. [En línea]. Monografía. Universidad de Chile. Santiago, Chile. 2011. [07.06.2021]. Disponible en: http://repositorio.uchile.cl/tesis/uchile/2011/ec-aviles_e/pdfAmont/ec-aviles_e.pdf

En conclusión, en este punto, se denomina una autentificación fuerte y segura, que incluye por lo menos dos de tres de los métodos mencionados anteriormente, siendo muy frecuente la autentificación biométrica, que como se indica anteriormente es la utilización de algún rasgo físico para la seguridad.

- **Confidencialidad:**

Es la propiedad de la seguridad que permite mantener en secreto la información y solo determinados usuarios pueden acceder a esta y manipularla.

Con el fin de evitar que nadie no autorizado pueda tener acceso a la información, se utilizan técnicas de cifrado o codificación de datos.

Se debe mantener una coherencia que permita determinar cuál es el nivel de confidencialidad de la información, esto para evitar un esfuerzo adicional a la hora de codificar una información que ya fue previamente codificada.

- **Integridad:**

La integridad de la información basa su accionar en lograr que la información que es trasmitida entre dos entidades (personas, entidad o máquina) no vaya a ser modificada por un tercero y esto se hace efectivo a partir de la utilización de firmas digitales; mediante este mecanismo, se codifican los mensajes que se van a trasferir, de forma que la función denominada hash, calcule un resumen de tal mensaje y lo añada al mismo.

Mantener la integridad de la información es importante para verificar que mientras esta viaja por la red no será modificada.

- **No-repudio:**

Este tipo de servicios le ofrecen al usuario una prueba de que la información fue entregada y una prueba al receptor del origen de la información que fue recibida.

Con este mecanismo, se busca que, una vez enviado el mensaje, la persona que lo envía no pueda decir que no es el autor original del mismo, pues quedará la prueba de que fue él quien lo realizó; esto se aplica también al receptor, quien no puede asegurar que no recibió el mensaje.

Lo anterior es importante para el comercio electrónico pues es una garantía para la realización de transacciones a través de plataformas electrónicas.

Tabla 1. Mecanismos de seguridad

Mecanismo de seguridad	Descripción	Ventaja
Autentificación	Proceso mediante el cual se verifica la identidad de las entidades que intercambian información.	Es uno de los mecanismos más seguros, el riesgo de suplantación es muy bajo.
Confidencialidad	Permite mantener en secreto la información, solamente ciertas personas pueden tener acceso a ella.	Permite la coherencia entre los receptores de la información y quienes la envían inicialmente.
Integridad	Evita que la información se manipulada por un tercero a partir del uso de firmas digitales.	Mediante la codificación de la información, mitiga el riesgo de modificación.
No repudio	Garantiza la correcta entrega de la información y emite una prueba de ello.	Se emite una constancia que garantiza la identidad de quien envía la información.

Fuente: Elaboración propia.

Como conclusión, teniendo en cuenta el cuadro comparativo realizado, se puede afirmar que es necesario incluir de dos a tres mecanismos de los anteriormente mencionados para garantizar un alto grado de seguridad en las transacciones electrónicas.

Mecanismos de seguridad en el comercio electrónico:

A medida que aumentan las compras por internet, también aumentan los delitos informáticos que se cometen para robar datos e información que los usuarios suministran en diferentes plataformas.

Según cifras de la AMVO, el comercio electrónico creció un 81% en 2020, lo que para los expertos significa que el usuario está dando más valor a la economía digital y más precisamente al comercio electrónico y todo lo que esto puede representar para la economía de los países alrededor del mundo.[25]

[25] RIQUELME, Rodrigo. E-commerce. Periódico El Economista. [En línea]. México. 2021. [Bogotá, junio de 2021) Disponible en: https://www.eleconomista.com.mx/empresas/Comercio-electronico-crecio-81-en-2020-asegura-AMVO-un-regreso-a-2016-segun-datos-de-la-Asociacion-de-Internet-20210127-0081.html

Teniendo en cuenta lo anterior y lo necesario que se ha hecho para los comercios implementar mecanismos de seguridad a sus plataformas, existen varios mecanismos de seguridad que permiten de un modo u otro blindar los datos que los usuarios registran en las diferentes páginas y aplicaciones web.

- Cifrado:

Garantiza que la información no es inteligible para individuos, entidades o procesos que no han sido autorizados, lo que se denomina privacidad.

El cifrado es la mutación de la información a una forma que solo es entendible utilizando una clave decodificadora.

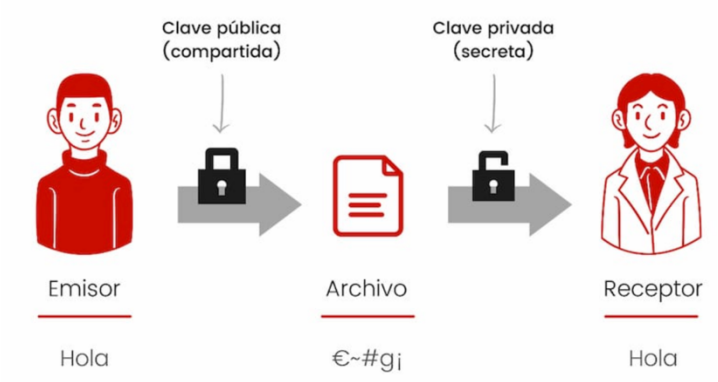
Cuando la información es cifrada se asegura que es auténtica, confidencial e integra.

Criptografía asimétrica:

Emplea claves para el envío de mensajes y pertenece a la persona a la que se le envía el mensaje, una clave es pública y la otra es privada.

La siguiente figura describe el proceso de la criptografía simétrica y las partes que intervienen.

Figura 1: Criptografía asimétrica.



Fuente: https://protecciondatos-lopd.com/empresas/criptografia-asimetrica/

Criptografía simétrica:

Se emplea una clave para la transformación del mensaje o de la información cifrada, tanto el emisor como el receptor deben conocer la clave.

La siguiente figura detalla el proceso de cifrado usado en la criptografía asimétrica.

Figura 2: Criptografía simétrica.

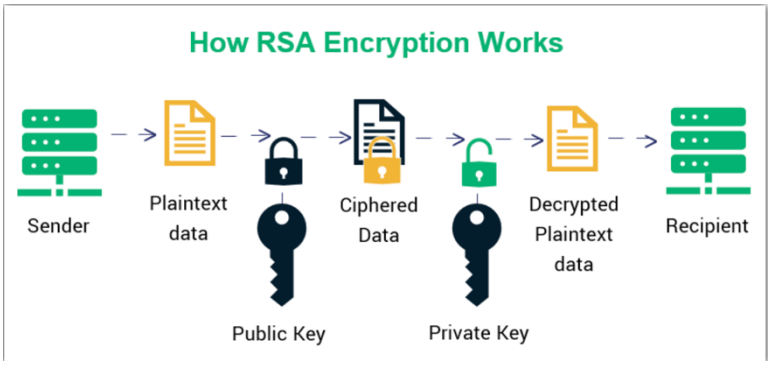
Fuente: https://securityhacklabs.net/articulo/criptografia-simetrica-asimetrica-e-hibrida

RSA:

Es el método más conocido de cifrado de la información, presenta todas las ventajas de los códigos asimétricos, incluye la firma digital y se basa en factorizar número muy grandes.

En la figura 3 representa el proceso para el cifrado de información a través del método RSA.

Figura 3: RSA.



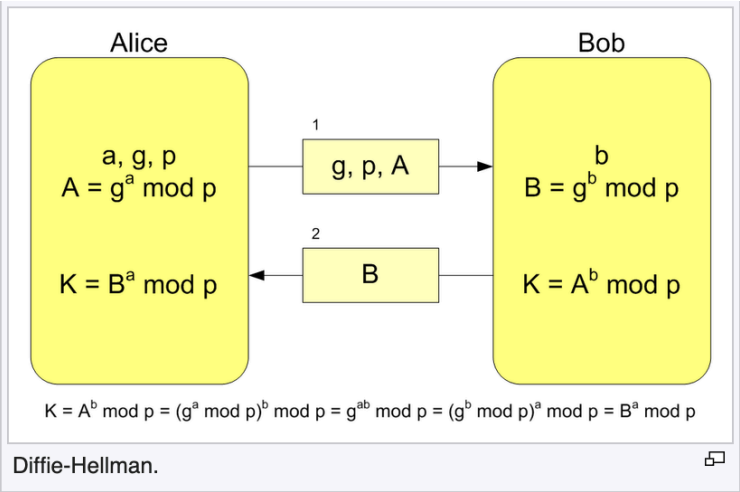
Fuente: http://seguridadinformatica-umex.blogspot.com/p/cifrado.html

Diffie-Hellman:

Este sistema inició los sistemas asimétricos y se basa en al algebra lineal. Fue el primer sistema de cifrado poli alfabético y era práctico para trabajar con más de 3 símbolos al tiempo.

La figura 4 precisa el funcionamiento del sistema Diffie-Hellman para el cifrado de información.

Figura 4: Diffie-Hellman.



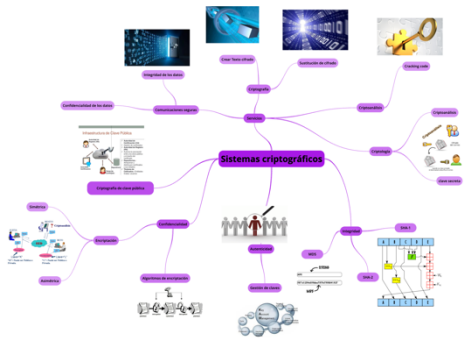
Fuente: https://es.wikipedia.org/wiki/Diffie-Hellman

Criptoanálisis:

Este método se usa para descifrar sin conocer las llaves, no se tiene ninguna información acerca del mensaje. Con el fin de evitar posibles ataques se debe conocer el diseño y las propiedades del sistema.

La siguiente figura puntualiza el funcionamiento detallado del criptoanálisis y las partes que intervienen en el.

Figura 5: Criptoanálisis.



Fuente: https://www.goconqr.com/en/p/14407195?canonical=true&frame=true&no_cache=true

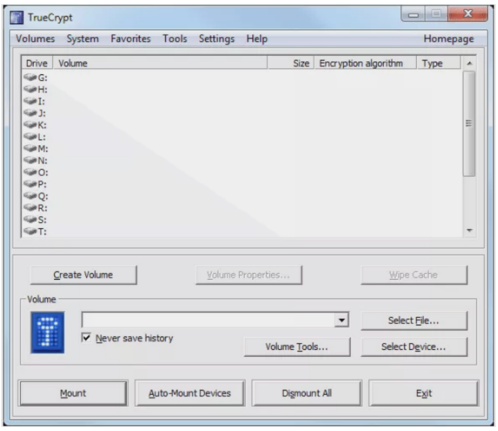
Herramientas para cifrar:

Truecrypt:

Este programa puede cifrar un texto, un archivo, una partición o un disco de almacenamiento como USB o disco duro.

En la figura 6 se observa la interfaz gráfica del software Truecrypt

Figura 6: Truecrypt.



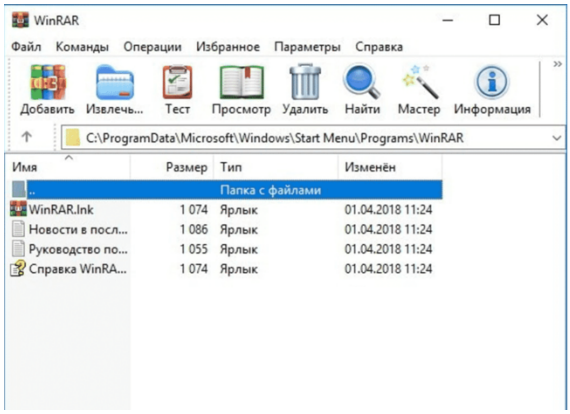
Fuente: https://www.lifewire.com/free-full-disk-encryption-programs-2619180

WinRAR:

Desarrollado por RARLAB que permite comprimir o cifrar cualquier tipo de archivo, en este cifrado se permite incorporar alguna clave, sin esta no será posible el descifrado del archivo.

De acuerdo con lo anteriormente mencionado en la siguiente imagen se puede apreciar la interfaz gráfica del software en mención.

Figura 7: WinRAR.



Fuente: https://softmany.com/es/winrar-windows/

- **Firmas digitales**

Una firma digital es un mecanismo criptográfico que realiza una función similar a la de las firmas escritas. Este mecanismo se utiliza para verificar la identidad del emisor del mensaje y de que el contenido del mensaje no ha sufrido ninguna alteración.

Desde el punto de vista normativo, el origen de estos mecanismos se planteó primero en las naciones unidas para reglamentar el derecho mercantil, mediante la expedición de la Ley Modelo sobre comercio electrónico. En esta ley se consagró el concepto de firma electrónica de tal modo que esta pudiera reemplazar la firma manuscrita.[26]

[26] PORTAFOLIO. [Sitio web]. Bogotá. Sección economía; todo lo que debe saber sobre firma electrónica. [15.06.2021]. Disponible en: https://www.portafolio.co/economia/todo-lo-que-tiene-que-saber-sobre-firma-electronica-y-firma-digital-541460

La firma digital, permite cumplir con ciertos requisitos legales y normativos muy exigentes que ofrecen altos niveles de seguridad sobre la identidad del firmante y da certeza sobre la autenticidad de los documentos que se firman.

Estos mecanismos, usan un ID digital basado en un certificado que emite una autoridad de certificación que es acreditada por proveedores de servicios de confianza.

Entonces, se analizan 4 puntos que hacen de la firma digital un mecanismo tan seguro:

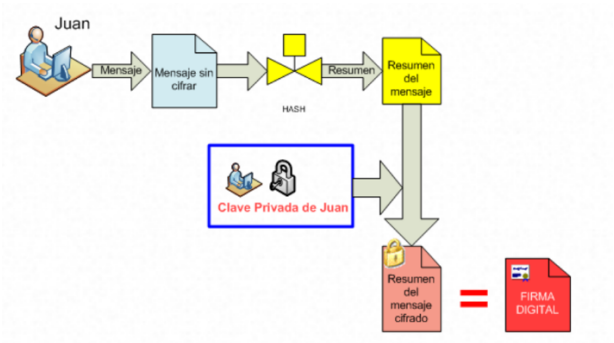
Confiable: los id provienen de certificados válidos de proveedores acreditados.
Todo está cifrado: tanto la firma digital como el documento que se firma se cifran y se vinculan a un sello de garantía.

Propia: cada vez que se firma un documento, se utiliza el certificado propio digital y PIN que es exclusivo para validar la identidad del firmante.

Validación: es muy fácil de validar por medio de una CA o de un TSP.

En la siguiente figura se puede apreciar como el emisor envía el mensaje sin cifrar; posteriormente este recibe un resumen del mensaje aplicando una función denominada ***función Hash***. Seguido a esto, el emisor cifra el resumen del mensaje utilizando la clave privada, obteniendo finalmente la firma digital del emisor.

Figura 8: Envío del mensaje firmado.

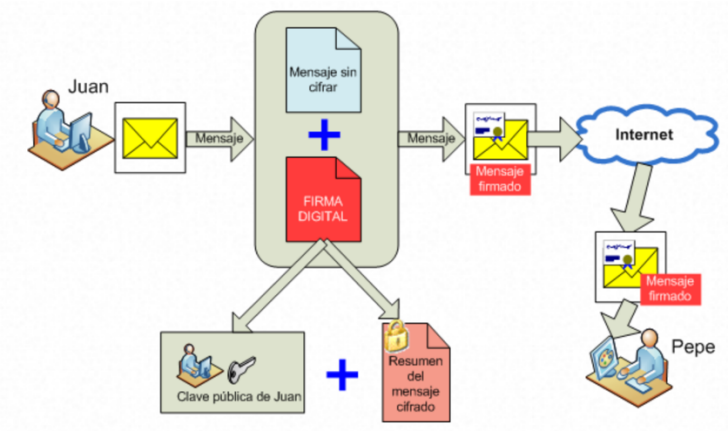


Fuente: https://www.descom.es/correo-electronico/firma-digital/como-funciona-una-firma-digital.html

En la siguiente figura se detalla como el emisor envía al receptor el correo electrónico, con la siguiente información:

- Contenido del mensaje: en texto plano y sin ser cifrado.
- Firma digital: que a su vez contiene el **resumen cifrado** mediante la clave privada y **el certificado digital** con los datos personales y la clave publica; estos datos deben estar cifrados por la entidad que provee el certificado.

Figura 9: Envío del correo electrónico.



Fuente: https://www.descom.es/correo-electronico/firma-digital/como-funciona-una-firma-digital.html

El emisor envía al receptor el correo electrónico cifrado y firmado.

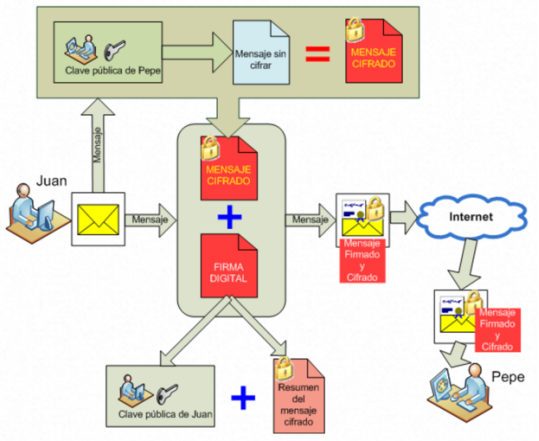
El emisor aparte de firmar el documento también debe cifrar el mensaje, de este modo solo podrá ser abierto y leído por el destinatario.

Para cifrar el mensaje se debe usar la clave pública del receptor que este ha enviado con el certificado digital. En este correo se debe tener la siguiente información:

- Contenido del mensaje cifrado, con la clave pública del receptor.
- Firma digital: con el resumen cifrado y el certificado digital.

Este proceso se detalla en la figura expuesta a continuación:

Figura 10: Mensaje firmado y cifrado.



Fuente: https://www.descom.es/correo-electronico/firma-digital/como-funciona-una-firma-digital.html

Por último, se debe verificar la firma digital del mensaje, para esto es necesario descifrar el certificado digital del emisor mediante la clave pública entrega la entidad certificadora, tal como lo muestra la figura 11 a continuación.

Cuando el certificado sea descifrado se puede acceder a las claves y a los datos de identificación de quien emite el mensaje o correo.

Figura 11: Mensaje firmado y cifrado.

Fuente: https://www.descom.es/correo-electronico/firma-digital/como-funciona-una-firma-digital.html

- **Certificados digitales**

Son archivos que identifican inequívocamente a un individuo o página web y permite establecer comunicaciones seguras y totalmente confidenciales. Se asocia el nombre de una entidad que participa en determinada transacción con la llave pública usada para firmar la comunicación con esa entidad en un sistema criptográfico.

Es el único medio que permite garantizar de manera técnica y legal la identidad de una persona en internet. Es un requisito indispensable en las entidades que deseen ofrecer servicios seguros a través de internet. El certificado digital permite cifrar las comunicaciones, significa que solamente el receptor final puede acceder al contenido de este. Entonces, la ventaja de los certificados digitales es que permite el ahorro de dinero y de tiempo al momento de realizar trámites por internet sin importar la hora y el lugar.

El certificado digital consta de claves criptográficas, una pública y una privada, que fueron creadas por medio de algoritmos matemáticos, de tal forma que la clave cifrada solo se puede desbloquear con su clave pareja.

- **Secure Socket Layer SSL**

Desarrollado por Netscape, proporciona autenticidad y privacidad de la información entre extremos sobre internet mediante el uso de la criptografía.

Es una tecnología que permite cifrar el tráfico de datos entre un navegador web y un sitio web, de esta forma se protege la conexión. De esta forma se impide que un hacker pueda visualizar o interceptar la información que es transmitida de punto a punto y que pueda incluir datos personales o financieros.

El protocolo SSL cifra y protege los nombres de usuarios y también las contraseñas, del mismo modo los formularios que se emplean en las diferentes páginas web para el envío seguro y autentico de datos personales, documentos o imágenes.

- **Firewalls**

Se definen como software o hardware que permiten que solamente los usuarios externos que cumplen con ciertas características y ciertos requisitos accedan a una red privada. Generalmente estos mecanismos permiten que los usuarios internos tengan un acceso total y completo a los servicios externos, mientras que se restringe el acceso exterior basándose en una serie de reglas.

Se establecen claves entre el ordenador que se conecta y el servidos utilizado para que la información viaje cifrada entre los dos sistemas, de esta forma si en algún

punto durante el viaje de la información se detecta algún elemento que pueda espiarlo, la información será inteligible.

4.2. MARCO CONCEPTUAL

La seguridad de la información consiste en asegurar que los recursos del sistema de información de determinada empresa se utilicen de la forma que esta lo ha decidido previamente y que el acceso a esta información se haga como la empresa u organización lo predispuso en un inicio, que las personas que acceden y manipulan la información hayan sido previamente autorizadas por el ente regulador de la empresa, evitando así posibles plagios o robos de la información.

Según la ISO27001, la seguridad de la información se refiere a la confidencialidad, la integridad y la disponibilidad de la información, así como de los datos importantes para la organización, sin importar el formato que tengan. [27]

La seguridad en la información tiene como único objetivo proteger los activos de información, estos activos están conformados por tres elementos:

- **información:** es el objetivo que representa un mayor valor para la empresa.
- **Equipos:** estos pueden ser software, hardware y de por si la propia organización**.**
- **Usuarios:** son todas las personas que hacen uso de la tecnología dentro de la organización.

El activo más importante que la empresa tiene es la información que le ha sido enviada por parte de sus clientes y/o usuarios, por ello es obligación de la organización contar con técnicas que aseguren y preserven la integridad y confidencialidad de estos datos; esta seguridad se genera colocando barreras, creando e implementando mecanismos, estrategias o procedimientos para resguardar el acceso y restringirlo a aquellas personas que no han sido autorizadas. Algunos medios necesarios para esto son:

- Restricción del acceso: de todas aquellas personas que forman parte de la organización y a los archivos más sensibles.

[27] SISTEMAS DE GESTION DE SEGURIDAD EN LA INFORMACIÓN. [Sitio web]. Bogotá. Blog especializado. [15.06.2021]. Disponible en: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

- Es importante y obligatorio asegurar que los operadores o personas autorizadas pueden realizar su trabajo asignado, pero no pueden incurrir en modificaciones en los programas o archivos sin que esto sea autorizado y sobre todo necesario.
- Se debe asegurar la utilización de los datos, archivos y todos aquellos programas correctos en todos y cada uno de los procedimientos que han sido elegidos.
- Se debe velar porque la información que sea transmitida sea la misma que será recibida por el destinatario.
- Organizar a todos los trabajadores y asignarles sus claves correspondientes, de tal forma que estas sean personales e intransferibles.
- Se debe actualizar todo de manera constante, esto incluye las contraseñas o códigos de acceso a los sistemas.

Lo primero que se debe hacer para poner en marcha la seguridad informática dentro de determinada organización es asegurar todos los derechos y claves para acceder a los datos y recursos que hacen parte de los activos de una empresa, establecer además las herramientas de control con las que se contará y los mecanismos para identificación. [28]

Así como es vital que la empresa cuente con un adecuado sistema de seguridad de la información, es importante y obligatorio que se realice un análisis previo de los posibles riesgos de la seguridad de la información y cuáles pueden ser sus consecuencias.

Entonces, una amenaza cibernética, se define como cualquier evento que pueda afectar los activos de información y está directamente relacionada con recursos humanos, eventos naturales, fallas técnicas. Algunos ejemplos de amenazas son: ataques informáticos externos, infecciones con malware, una posible inundación, un incendio, un terremoto o un corte en el fluido eléctrico.

Por lo anterior, se debe realizar una adecuada gestión y análisis del riesgo, esto va a permitir a la empresa conocer cuáles son las posibles vulnerabilidades a los que están sujetos sus activos de información. Dicho esto, un correcto y riguroso proceso de identificación de riesgos implica:

[28] SISTEMAS DE GESTION DE SEGURIDAD EN LA INFORMACIÓN. [Sitio web]. Bogotá. Blog especializado. [15.06.2021]. Disponible en: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

- Identificar cuáles son todos aquellos activos de información que significan un valor importante para la empresa.
- Asociar las posibles amenazas a los activos previamente identificados.
- Determinar cuáles son las posibles vulnerabilidades que pueden ser aprovechadas por tales amenazas.
- Identificar y medir el impacto que podría generar el hecho de sufrir una pérdida en la confidencialidad, integridad y disponibilidad de cada activo.

Son varios los retos a los que se enfrentan las empresas que alrededor de la seguridad de la información:

Actualización constante: la tecnología avanza rápidamente, es decir que pone a prueba los conocimientos y obliga a empresas y usuarios a ir a la par de ellos, cualquier retraso en cuanto a conocimientos se refiere, puede significar pérdidas millonarias, es por esto que las empresas deben disponer de un equipo especializado que esté en constante actualización y modernización en los mecanismos de seguridad de las instituciones.

Capacitación al personal: La seguridad de la información es una responsabilidad de todo el personal, y esto involucra a todos los trabajadores sin importar su jerarquía o cargo dentro de la empresa. De este modo, la empresa adquiere una obligación al tener que invertir en capacitación y conocimiento a sus trabajadores, de este modo se garantizan altos niveles de seguridad. [29]

En consecuencia, es necesario analizar el impacto del negocio de la empresa si un posible fallo de la seguridad llegase a ocurrir, generando una pérdida en la confidencialidad, que como lo he mencionado antes es uno de los atributos de la seguridad en la información; se debe evaluar de manera muy realista y ligados a escenarios reales la probabilidad de que estos eventos desafortunados pueden ocurrir, de este modo se debe prever las amenazas, vulnerabilidades e impactos.

Un ejemplo de una correcta metodología para la evaluación y análisis de estos riesgos tendría las siguientes fases:

1. Recopilación y preparación de toda la información.

[29] IBERO CIUDAD DE MEXICO. [Sitio web]. México. La importancia de la seguridad de la información. [15.06.2021]. Disponible en: https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

2. Identificación, clasificación y valoración de los grupos de activos que hacen parte de la información de la organización.
3. Identificación y clasificación de las amenazas.
4. Registro y estimación de las vulnerabilidades.
5. Diferenciación y valoración de los posibles impactos, lo que incluye: identificar, tipificar y valorar tales impactos.
6. Evaluación y análisis completo y concienzudo del riesgo.

La implementación de métodos electrónicos para adquirir bienes y servicios por parte de los comercios se ha tenido que regular por parte de los gobiernos y de los demás entes reguladores encargados; de este modo se han creado e implementado ciertas normas o estándares de seguridad con el propósito de facilitar el comercio, el intercambio de información y contribuir a la transferencia de diversas tecnologías.

Las normas ISO/IEC 27000:2013, son un conjunto de estándares de seguridad que ya están desarrollados en su mayoría o que están en fase de desarrollo y que proporcionan un marco para la gestión de la seguridad; contienen las mejores prácticas recomendadas en seguridad de la información con el fin de desarrollar, implementar y mantener ciertas especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), que es utilizable y apta para cualquier tipo de comercio, privado o público, pequeño o grande. La seguridad de la información, según la norma ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad.

Cada vez son más las empresas que disponen de plataformas electrónicas como medios de pago para sus clientes, de este modo ha aumentado la adquisición de bienes y servicios desde la web. A continuación, se mencionan y analizan brevemente los diferentes métodos de pago electrónico que existen el mercado actualmente.

- **Tarjeta bancaria:** es el método de pago más popular dentro del comercio electrónico y han sido muchos los esfuerzos por parte de las empresas y/o organizaciones para ofrecer seguridad y fiabilidad en el uso de estos plásticos. Las tarjetas bancarias tienen 3 usos dentro del comercio electrónico.

Por un lado, la emisión de la orden de pago y luego la comunicación de los datos de la tarjeta, ya sea por vía telefónica o fax; la emisión de una orden de pago a

través de un formulario web por medio de un canal que debe estar protegido y finalmente la emisión de una orden de pago por medio de un formulario web con una conexión segura y cuyos datos deben ir totalmente cifrados.

En cuanto a los usos, es válido decir que el primero ya desapareció por arcaico e inútil. El segundo originó gran avance en el desarrollo de diversos sistemas de pago.

La principal ventaja del uso de las tarjetas bancarias es que permite realizar el pago como si el cliente tuviese el dinero en las manos, un dinero en efectivo, y una de las desventajas que las entidades han identificado es la incompatibilidad de algunas franquicias con las plataformas de pago y en algunas ocasiones el robo de datos por medio de fraudes. [30]

- **Dinero electrónico:** no es otra cosa sino el supuesto del dinero, no hay papel y en su lugar el dinero está contenido en bits y correctamente cifrado.

Algunas ventajas son:

- ✓ La aceptación universal del dinero electrónico como medio de pago.
- ✓ Paga garantizado que no depende de la existencia de la cuenta de un tercero.
- ✓ No se genera ningún costo para el usuario.
- ✓ Es totalmente anónimo.

- **Pago mediante teléfonos móviles:** el auge del uso de teléfonos móviles en la generación actual y el hecho de que actualmente las personas que cuentan con estos elementos prefieran hacerlo todo desde allí, ha obligado a las empresas telefónicas a crear sistemas de pago rápido y seguros. Es una alianza entre las empresas telefónicas, el usuario, el banco donde el usuario tenga sus cuentas y dinero y el comercio donde el cliente decida comprar determinado articulo o adquirir determinado servicio.

[30] QONTO. Ventajas y desventajas del uso de tarjetas de crédito. [Sitio web]. Lima. [16.06.2021]. Disponible en: https://qonto.com/es/tips/payment-methods/ventajas-y-desventajas-de-las-tarjetas-de-credito-y-debito

Sistemas de pago por internet

- **PayPal:** es una empresa del grupo eBay y es la empresa líder en soluciones de pago por internet. Este método de pago permite:

✓ Pagar compras realizadas en determinada página web.
✓ Recibir el pago de ventas realizadas en determinada tienda de internet.
✓ Enviar y recibir dinero.

Este método fue creado para competirle a las tarjetas de crédito ya existentes; permite hacer pagos sin necesidad de dar el número de la tarjeta de crédito lo que genera una gran ventaja para los más de 40 millones de usuarios que tiene PayPal actualmente. Es una modalidad de pago segura, gratuita, fácil, rápida, cómoda e internacional, tanto para vendedores como para compradores. Las estadísticas muestran que las transacciones por PayPal aumentaron en un 105% en los últimos 3 años, para el segundo trimestre del 2020, el total de usuarios ascendía a 346.[31]

El gerente general de PayPal en América Latina, asocia el incremento de las transacciones por este medio a la pandemia originada por el Covid19, y argumenta que "La gente que hoy siente animadversión por el uso del dinero en efectivo por lógicas razones higiénicas, sigue explorando aplicación de pago electrónico, las tiendas físicas exploran modelos para mantener las ventas"[32]

- **PSE:**

Otro de los medios de pago que más se ha consolidado es el pago en línea PSE, un botón de pagos totalmente seguro y en línea; un servicio de ACH Colombia que le permite a las empresas vender o recaudar a través de internet, a través de este botón los clientes o usuarios autorizan mediante la sucursal virtual de su banco el débito automático de sus cuentas, ya sea de ahorros o corrientes. Es válido recordar que ACH Colombia es una compañía que brinda servicios tecnológicos a los

[31] CIO INFORMACION Y ESTRATEGIA. Transformación digital. [Sitio web]. Brasil. [16.06.2021]. Disponible en: https://thestandardcio.com/2020/09/16/las-transacciones-de-paypal-se-disparan-105-en-tres-anos/#:~:text=Las%20estad%C3%ADsticas%20muestran%20que%20el,un%20105%25%20en%20tres%20a%C3%B1os.&text=Hace%20cinco%20a%C3%B1os%2C%20PayPal%20ten%C3%ADa,el%20segundo%20trimestre%20de%202020.

[32] GOMEZ Federico. PayPal, pagos y comercio electrónico se aceleran en América Latina. [Sitio web]. México. [16.06.2021]. Disponible en: https://thestandardcio.com/2020/06/11/paypal-pagos-y-comercio-electronico-se-aceleran-en-latinoamerica/

colombianos con el fin de mejorar la calidad de vida, es una organización regulada y vigilada por la Superintendencia Financiera y sus principales accionistas son las entidades bancarias y financieras del país.

En cuanto a la seguridad, Gustavo Vega, presidente de ACH Colombia afirma que, la seguridad en PSE no es solamente un concepto técnico, es el espíritu que mueve toda la operación, se cree que, bajo ambientes seguros, se desarrollan grandes competencias de construcción y colaboración. [33]

Entre las ventajas que el uso del pago por PSE ofrece a las empresas, podemos ver:

- ✓ Agilidad en los recaudos de dinero
- ✓ Facilidad para actualizar la información
- ✓ Información en línea sobre los recaudos
- ✓ Oportunidad de manejo óptimo de los inventarios
- ✓ Agilidad en la conciliación de las transacciones
- ✓ Reducción en costos
- ✓ Seguridad en el manejo de la información y el dinero

A continuación, el lector puede encontrar un cuadro comparativo con la descripción y ventajas entre los métodos de pago electrónico anteriormente mencionados:

Tabla 2. Medios de pago electrónicos

Medio de pago electrónico	Descripción	Como funciona	Características / ventajas
PayPal	Es una empresa del sector del comercio electrónico, cuyo sistema permite a los usuarios, realizar pagos y transferencias a través de internet sin tener que	El envío de dinero o pagos a través de esta plataforma es gratuito. 1. Se elije la opción de pago (tarjeta crédito o débito, saldo en	• Servicio gratuito, sin comisiones o cuotas. • No se deben suministrar los datos de las

[33] VEGA, Gustavo. ACH COLOMBIA, la seguridad en pse. [Sitio web]. Bogotá. [16.06.2021]. Disponible en: https://www.pse.com.co/web/guest/persona-la-seguridad-en-pse

	compartir la información financiera con el destinatario.	PayPal, cuenta bancaria) 2. Se realiza el envío del dinero sin compartir información. 3. El destinatario recibe el mensaje.	tarjetas usadas para el pago. • Compras protegidas hasta por 1000 EUR, por políticas del proveedor.
PSE	Es un sistema de pagos, que permite al usuario realizar pagos por internet.	El uso de esta plataforma es totalmente gratuito. 1. Se crea un usuario con clave y contraseña. 2. La plataforma re direcciona al usuario a la página del banco donde tiene su cuenta bancaria. 3. Se realiza el débito desde la cuenta bancaria.	• Servicio gratuito. • Puede hacer pagos desde la comodidad de su hogar u oficina. • Mayor seguridad, agilidad y confianza. • Pagos más fáciles y sin usar efectivo.

Fuente: elaboración propia

Finalmente, y luego de ver y analizar los diferentes medios de pago electrónicos que existen actualmente, es válido hablar acerca de las vulnerabilidades que tiene el comercio electrónico. Es innegable el ascenso que ha tenido el e-commerce en Colombia y en el mundo, es un tipo de comercio lleno de oportunidades y que ha servido como escalón para aquellas personas que desean emprender con tiendas por internet, sin embargo, el uso de las diferentes plataformas de pago que ofrece el comercio electrónico tiene vulnerabilidades y genera ciertos riesgos por su uso. A continuación, mencionaré los cuatro ataques más comunes al e-commerce y como pueden ser mitigados:[34]

- ✓ **Fraude directo:** es la fuente de riesgo más común para un comercio electrónico, y también es la más difícil de controlar. Las técnicas de robo y fraude son cambiadas constantemente por los ciberdelincuentes y es todo un reto para las

[34] SWHOSTING. Seguridad E-commerce. [Sitio web]. Medellín. Los 4 ciber ataques más comunes al comercio electrónico. [16.06.2021]. Disponible en: https://www.swhosting.com/blog/seguridad-ecommerce-los-4-ataques-mas-comunes/

entidades competentes en el tema mantenerse al día y actualizados para evitarlo.

Tarjetas de crédito robadas: este tipo de fraude se encuentra en cualquier comer electrónico y el objetivo no es otro que tener acceso al producto antes de que el comercio detecte que esta tarjeta es robada. Es muy peligroso para los e-commerce que ofrecen productos digitales y que deben hacer entregas inmediatas al cliente.

La mejor forma de mitigar este tipo de fraude, especialmente para comercios pequeños y medianos es hacer uso de la pasarela TPV que ofrece el banco, pues de esta forma toda la responsabilidad recaerá sobre el banco y será esta entidad la encargada de validar la tarjeta.

Devolución forzosa: esto ocurre cuando la entidad bancaria del usuario o cliente realiza la sustracción de un cobro recibido, esto pasa generalmente cuando se ha aceptado una compra fraudulenta. Sin embargo, hay dos escenarios más en los cuales se realizar devolución forzosa, veamos:

A través de PayPal o proveedores parecidos: cuando un estafador asocia una tarjeta robada a su cuenta de PayPal y hace compras sin levantar ni la más mínima sospecha. Pueden pasar 6 meses para que PayPal haga el reverso.

De forma voluntaria: es posible que el estafador use su tarjeta o cuenta de manera perfecta, posteriormente el cliente se comunica con el banco y manifiesta que esta compra fue hecha sin su consentimiento o que fue víctima del robo de la tarjeta.

Una vulnerabilidad en la web: este tipo de fraude se lleva a cabo aprovechando la vulnerabilidad que tiene el código de la página web; el estafador puede cambiar los precios de los productos, siempre reduciendo considerablemente su valor. Legalmente no es posible demostrar que esto se hizo de forma intencionada y que no fue un error, casi siempre el comercio debe asumir el costo, sin lugar a reclamos.

Para mitigar este tipo de ataque es importante que el comercio cuente con una página web que haya sido previa y exhaustivamente examinada, buscando sus vulnerabilidades, debe ser un grupo especializado y certificado en este tema y habilidades.

- ✓ **Robo de información:** es el tipo de ataque más grave y que más preocupa al comercio electrónico. Puede tener devastadoras consecuencias económicas, así como puede sufrir la sustracción de datos sensibles de los clientes y/o usuarios del comercio lo que puede arruinar la reputación y conllevar serias repercusiones legales.

  Expertos del área de seguridad del banco BBVA, brinda algunos consejos a sus usuarios, con el fin de proteger su información más sensible; algunos de estos son: [35]

  - Utilizar siempre un antivirus en los equipos y siempre mantenerlo actualizado.
  - Verificar que el sistema operativo y demás aplicaciones siempre estén actualizadas.
  - Usar siempre páginas https, pues mantiene conexiones cifradas, lo que asegura transacciones seguras.
  - Borrar periódicamente el historial y las llamadas cookies del ordenador.
  - Cuando se usen equipos ajenos siempre se debe usar el modo incognito de navegación y cerrar la sesión al terminar.
  - No manejar información personal cuando se esté conectado a redes wifi-públicas.

  Los números de tarjetas de crédito, contraseña e información personal hacen parte de la información que siempre busca robar el atacante, con el fin de usarlos en el mercado negro o suplantar al titular.

- ✓ **Phishing:** esto ocurre cuando un ciber delincuente crea una página web idéntica a la de nuestro comercio, esto puede incurrir en el daño a la reputación de nuestra tienda, el atacante busca robar la información de nuestros clientes por medio del engaño. Este tipo de ataque es más común en comercios electrónicos que ofrecen servicios financieros.

  El phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. [36]

---

[35] BBVA. Robo de información personal, ¿cómo puedo protegerme? [Sitio web]. Bogotá. [07.06.2018]. Disponible en: https://www.bbva.com/es/robo-informacion-personal-puedo-protegerme/

[36] ALWAREBYTES. Suplantación de identidad. [Sitio web]. Bogotá. [20.06.2020]. Disponible en: https://es.malwarebytes.com/phishing/

- ✓ **Ataques DDoS – Denegación del Servicio:** es uno de los ataques más comunes en la red, la denegación del servicio. Este ataque puede poner fin al negocio online durante horas o incluso días si no se cuenta con las herramientas necesarias para mitigarlo. El atacante usa un *botnet* que es una red de máquinas infectadas con el fin de lanzar peticiones de conexión al comercio, dado esto, el servidor no podrá solucionar todas las peticiones y el negocio quedará sin acceso durante el tiempo que el ataque dure. Por lo anterior es necesario que la empresa cuente con mecanismos que le permitan detectar y neutralizar estos ataques a cualquier hora del día. Dentro de los objetivos más comunes de los ataques DDoS se incluyen:[37]

    - Sitios de compra por internet.
    - Casinos en línea
    - Cualquier empresa u organización que dependa de la prestación de servicios en línea.

En conclusión, la empresa o comercio debe ser muy rigurosa a la hora de implementar los mecanismos que permita evitar, detectar y mitigar los diferentes ataques que pueden afectar sus transacciones electrónicas. Además de ello deben analizar los pro y contras que puede generar estos riesgos. La empresa debe generar al cliente confianza, esto le permitirá aumentar sus ingresos y posicionar su imagen en el mercado.

4.3. MARCO LEGAL

Debido al gran auge que ha tenido el comercio electrónico en Colombia y en el mundo, y debido a la gran cantidad de robos y delitos cometidos alrededor de las diversas plataformas que existen, se ha hecho necesario que los gobiernos creen e implementen leyes que permitan la regulación del comercio electrónico en muchos aspectos. En Colombia, existe la Ley de comercio electrónico, pues fue

[37] KAPERSKY. Ataque DDoS. [Sitio web]. Bogotá. [18.03.2019]. Disponible en: https://latam.kaspersky.com/resource-center/threats/ddos-attacks#:~:text=Los%20ataques%20de%20red%20distribuidos,distribuida%20de%20servicio%20(DDoS).&text=El%20ataque%20DDoS%20env%C3%ADa%20varias,evitar%20que%20este%20funcione%20correctamente.

implementada para aumentar la confianza entre las empresas que ofrecer productos a través de plataformas electrónicas y quienes prefieren este tipo de sitios web para realizar pagos y adquirir servicios.

- ✓ **Ley 527 de 1999, Ley de comercio electrónico en Colombia (Legislación Nacional – Colombia)**

La presente ley será aplicable a todo tipo de información que sea emitida en forma de mensaje de texto, salvo en los siguientes casos:

- En las obligaciones contraídas por el Estado colombiano en virtud de Convenios o Tratados internacionales.
- En las advertidas escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

En su parte 3, la presente norma trata sobre *las firmas digitales, certificados y entidades de certificación,* que como lo vimos son mecanismo que permiten asegurar la información que es relacionada en determinada plataforma electrónica al momento de adquirir un bien o servicio.

El capítulo I, reglamenta las firmas digitales y las atribuye de la siguiente forma "*cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido de este",* lo anterior quiere decir que da por entendido que la persona que firma el mensaje será quien quede vinculado totalmente con el contenido de este.

Además, dicha ley establece que una firma digital tiene la misma fuerza y mismos efectos que una firma manuscrita, siempre que esta tenga los siguientes atributos:

- Es única a la persona que la utiliza.
- Es susceptible y permite ser verificada cuando sea necesario.
- Esta bajo el control exclusivo de la persona que hace uso de esta.
- Está ligada a la información o al mensaje, de tal modo que, si este mensaje o información son modificadas total o parcialmente, la firma dejará de ser válida.

- La firma esta creada conforme a todas las disposiciones y reglamentaciones dispuestas por el Gobierno Nacional.

En Colombia, la ley que se encarga de la regulación y aclaración del comercio a través de canales digitales recibe el nombre de ***Ley de Comercio Electrónico***, esta ley se creó con el fin de proteger a los compradores digitales y a las comercios y personas naturales que desean poner sus productos y servicios a disposición del público a través de plataformas web, aplicaciones móviles y redes sociales. [38]

✓ **Marco regulatorio:**

Esta ley cuenta con un marco regulatorio que busca proteger y blindar el derecho fundamental a la iniciativa privada y al libre desarrollo de esta. Es una ley que protege, pero al mismo tiempo exige tanto a los comerciantes como a los consumidores digitales, dentro de esta regulación se destacan tres puntos importantes:

1. La libertad de empresa: es el derecho que tienen todos los colombianos a emprender, sin embargo, para crear empresa en el territorio colombiano, ya sea e-commerce o comercio tradicional en establecimiento comercial, tiene unos deberes que deben ser cumplidos, tal como el pago de impuestos y la certificación obligatoria de una firma electrónica.

2. El buen nombre: todos los colombianos, vendedores y compradores de bienes y servicios tienen derecho al buen nombre. Para el caso del comercio electrónico, que la presentación de la empresa y ofrecimiento de artículos o servicios se hace por medio de redes sociales y demás canales digitales, el proceso de venta no debe afectar la dignidad de quien vende o quien compra.

3. Los datos: durante todo el proceso de la venta digital de determinado articulo o adquisición de tal servicio, se exponen datos privados y financieros, que, dentro de la clasificación de datos, se ubican como datos sensibles. Los consumidores

[38] J4PRO. Ley de comercio electrónico en Colombia. [Sitio web]. Bogotá. [16.06.2021]. Disponible en: https://j4pro.com/ley-de-comercio-electronico-en-colombia#:~:text=La%20Ley%20527%20de%201999,firma%20aut%C3%B3grafa%20y%20firma%20electr%C3%B3nica.&text=Esta%20Ley%20tambi%C3%A9n%20es%20la,competentes%20para%20realizar%20esta%20certificaci%C3%B3n.

tienen el derecho a conocer tal información. Por otro lado, las empresas están en la obligación de proteger y no comercializar estos datos.

- ✓ **Marco del consumidor:**

Pese a que en Colombia la ley de comercio electrónico acoge los derechos y las obligaciones de los empresarios, también involucra decretos que tiene como fin proteger al consumidor final.

1. Ley 1266 de 2008; allí se expone el régimen especial para servicios financieros. Dentro de esta ley se incluye la constitución de bases de datos con el objetivo de calcular el riesgo crediticio.
2. Decreto 1727 de 2009; ordena que sean presentados los datos de los titulares de la información, ya sea información crediticia, financiera, comercial, de servicios, incluyendo los datos que provienen de otros países.
3. Decreto 1377 de 2013; protege y garantiza el derecho que tienen los usuarios de conocer su información financiera y todas aquellas actualizaciones que se hagan en el trascurso del tiempo. [39]

- ✓ **Marco constitucional:**

Constitucionalmente son tres los artículos que contemplan las garantías de vendedores y compradores dentro del comercio electrónico.

1. Artículo 15 de la Constitución Política o Habeas Data: en este artículo se defiende el derecho a la intimidad personal, familiar y al buen nombre del individuo. Para el caso del e-commerce en Colombia, esta norma esta aplicada para ***las transacciones en las que las plataformas o canales de venta digital exijan datos personales y sensibles.***

2. Artículo 20 de la Constitución Política: este artículo protege la libertad de expresión. En cuanto al comercio electrónico es una garantía, pues se realizan ventas de forma no presencial y a audiencias con gustos no específicos.

[39] CCE. Cámara de comercio electrónico. Regulaciones del comercio electrónico. [Sitio web]. Bogotá. [16.06.2021]. Disponible en: https://www.ccce.org.co/

3. Artículo 333 de la Constitución Política: tal artículo protege la libertad de empresa en Colombia; la actividad económica de la misma, y la iniciativa privada son totalmente libres, dentro de los límites del bien común. Para tal ejercicio, nadie podrá exigir permisos previos y tampoco requisitos sin autorización de la ley.

✓ **Marco legal:**

El marco legal va direccionado a la implementación de medidas que hagan que el comercio electrónico contribuya al desarrollo y bienestar del estado colombiano, además prever que sea una actividad igualitaria.

Este marco está integrado por dos leyes:

1. Ley 527 de 1999, La Ley de comercio electrónico en Colombia: esta ley establece la equivalencia que hay entre la firma electrónica y la firma manuscrita, así mismo entre datos digitales y documentos escritos. Adicional, regula las reglas para la certificación de las firmas digitales y crea las entidades exclusivas que deben otorgar esta certificación. [40]

   Para la reglamentación de esta ley se considerará:

- Mensaje de datos: información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares.
- Comercio electrónico: abarca todas aquellas cuestiones suscitadas por toda relación de índole comercial que sea estructurada a partir de la utilización de mensajes y datos o cualquier medio similar.
- Firma digital: será el valor numérico que se adhiere al mensaje de datos y que vinculado a un procedimiento matemático garantizará que la información no sea modificada.
- Entidad de certificación: es aquella persona que está autorizada por la ley y tiene la facultad de emitir certificados con relación a las firmas digitales.
- Intercambio electrónico de datos: es la trasmisión electrónica de datos de un computador a otro, siempre debe estar estructurada bajo normas técnicas.

[40] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 de 1999. (16, junio, 2021) Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico. En: presidencia de la república de Colombia. Bogotá D.C. 2021. 2P.

- Sistema de información: es todo sistema utilizado para generar, enviar, recibir o procesar algún tipo de datos.

2. Artículo 91 de la Ley 633 de 2000: tal artículo ordena que las páginas web o sitios de internet que tengan origen en Colombia y que realizan determinada actividad económica, obligatoriamente deben estar inscritas en el Registro Mercantil y suministrar a la Dian toda la información que este ente regulador solicite. Esta ley en pocas palabras obliga a las empresas que son parte del comercio electrónico a pertenecer al régimen tributario sin ninguna excepción.[41]

4.4. ESTADO ACTUAL

A continuación, se realiza una pequeña radiografía y análisis del estado del comercio electrónico en Colombia y como se proyecta a estar dentro de un periodo de tiempo, lo anterior basándose en datos suministrados por Blacksip, una empresa que ofrece asesorías en e-commerce y en transformación digital en empresas colombianas y del mundo. [42]

Dentro de un análisis que desarrolló la empresa mencionada, se encuentran algunos datos, a continuación, los más relevantes:

- ✓ Colombia es uno de los países de América Latina con más proyección y éxito en las ventas digitales.
- ✓ Durante el 2016, el valor aproximado de las ventas realizadas por medio de canales digitales fue de US $26.700 millones.
- ✓ Entre el 2015 y el 2016 el e-commerce en Colombia tuvo un crecimiento del 64%.
- ✓ En 2016, el porcentaje de personas que compraron a través de plataformas digitales llegó al 76%, tuvo un crecimiento del 46% respecto al 2013.

[41] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 633 de 2000. (16, junio, 2021) Por medio de la cual se define y reglamenta el uso de las páginas web. En: presidencia de la república de Colombia. Bogotá D.C. 2021. 6P.

[42] BLACKSIP. REPORTE DE INDUSTRIA. El eCommerce en Colombia 2020. [Sitio web]. Bogotá. [18.06.2021]. Disponible en: https://content.blacksip.com/ebook-reporte-de-industria-el-ecommerce-en-colombia-2020?utm_term=ecommerce%20colombia&utm_campaign=ReporteIndustria_20_CO&utm_source=ppc&utm_medium=ppc&hsa_acc=7893706222&hsa_cam=11915677177&hsa_grp=119270823487&hsa_ad=505243177120&hsa_src=g&hsa_tgt=kwd-298316184141&hsa_kw=ecommerce%20colombia&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwwqaGBhBKEiwAMk-FtPA0JCRJIP7IZGrHOSeYkBUxxW9udINTkJY2nP8IS84DVtnvtg6hVxoC658QAvD_BwE

- ✓ Una semana de promociones en la web significa el 5.6% de las ventas totales de un comercio al año, mientras que, para el mismo comercio, en el mismo segmento del año solamente representa el 2% las ventas presenciales.
- ✓ Actualmente en Colombia las ventas por internet alcanzan entre el 1% y el 3% de las ventas totales, lo que es un gran número, por ejemplo, comparado con Inglaterra que alcanza el 12%.
- ✓ El nivel de fraude en transacciones electrónica en Colombia alcanza el 0.45%, se ubica por debajo de países como Perú con el 0.52% y México con el 1.5%.

En Colombia y Latinoamérica el comercio electrónico crece de gran manera, alcanzando un porcentaje de dos dígitos en el último año, los expertos aseguran que para finales del 2020 llegue al 17% de ventas totales, alcanzando la gran cifra de US $85.000 millones para el mes de diciembre. [43]

Los colombianos utilizan cada vez más el comercio electrónico, y su gran auge está asociado a varios factores como la facilidad, la comodidad y una mayor oferta de productos, además de la variedad y la seguridad que dicen encontrar en los diferentes medios de pago ofrecidos por los diferentes comercios, incluyendo el pago contra entrega y el pago por efecty o baloto, lo que genera más seguridad sobre el dinero del usuario.

Andrés Felipe Fuentes, country mánager de PayU Colombia considera que en Colombia se ha visto un gran interés por parte de las empresas por adoptar diversas formas de pago seguras y confiables a sus clientes, así mismo, Fuentes considera que el e-commerce está cada vez más cerca de las pymes.

Durante la actual crisis económica y sanitaria que vive el país a raíz de la pandemia del Covid19, el comercio electrónico ha sido uno de los sectores más importantes y relevantes en el desarrollo del país; pues debido a que muchas empresas tuvieron que cerrar sus puertas al público, adaptaron sus ventas y estrategias a los canales digitales y debieron trasladar sus transacciones al mundo virtual.

[43] LR. LA REPUBLICA. Comercio electrónico ha crecido más de 300% en Latinoamérica en pandemia. [Sitio web]. Bogotá. [16.06.2021] Disponible en: https://www.larepublica.co/globoeconomia/e-commerce-ha-crecido-mas-de-300-en-latinoamerica-en-medio-de-la-pandemia-3000424

Durante el 2019, las ventas a través del comercio electrónico crecieron en promedio 2.74%, mientras que para enero de 2020 el crecimiento fue de 1,9%. [44]

[44] CCE. CÁMARA DE COMERCIO ELECTRÓNICO. Comportamiento del eCommerce en Colombia durante el 2021. [Sitio web]. Bogotá. [16.06.2021]. Disponible en: https://www.ccce.org.co/wp-content/uploads/2020/10/informe-comportamiento-y-perspectiva-ecommerce-2020-2021.pdf

5. DESARROLLO DEL PROYECTO

IDENTIFICAR LOS DIVERSOS MECANISMOS Y ESTRATEGIAS PARA LA SEGURIDAD EN LAS TRANSACCIONES ELECTRÓNICAS QUE EXISTEN

Una transacción electrónica es la venta o compra de bienes o servicios, esta puede darse entre empresas, hogares, personas u organizaciones públicas o privadas que son realizadas a través de plataformas electrónicas por medio de dispositivos como celulares o computadores, entre otros. La mayoría de las transacciones realizadas son monitoreadas con el fin de garantizar la seguridad de la información de extremo a extremo.

Teniendo en cuenta el gran auge y desarrollo que ha tenido el comercio electrónico en el mundo; viendo que son cada vez más las personas que a diario prefieren realizar sus pagos, compras y demás transacciones por medio de aplicaciones virtuales y plataformas web y sin tener que salir de casa e ir a hacer filas en un almacén o en una entidad financiera con el fin de pagar la cuota de un crédito o el pago de un servicio público y según datos que da la CCE, 8 de cada 10 colombianos prefiere las plataformas electrónicas, por lo anterior, se evidencia la importancia de estas en el mundo moderno y globalizado en el que el ser humano se desenvuelve actualmente. [45]

El uso de las plataformas electrónicas para realizar pagos y la gran popularidad que ha tenido el dinero electrónico en los últimos tiempos se debe también al peligro que representa para una persona llevar consigo altas sumas de dinero en efectivo, reportes de la policía indican que el denominado fleteo es uno de los actos delictivos más comunes actualmente.

Un comercio, empresa u organización que ha decidido llevar sus productos o servicios a la web, con el fin de ofrecerlos a un grupo enorme de personas que están a tan solo un clic de distancia, no solo debe ofrecer una página amigable y en la que sea fácil navegar, sino que debe garantizar que será totalmente segura, de este modo no solo ofrecerá un buen servicio, también se posicionará como una marca confiable, aumentando sus clientes y/o usuarios y por ende sus ingresos.

[45] CCE. Cámara de comercio electrónico. [Sitio web]. Bogotá D.C. [20.06.2021]. Disponible en: https://www.ccce.org.co/noticias/

Por lo anterior, se reafirma la hipótesis y planteamiento previamente argumentado, de que la seguridad informática en las transacciones electrónicas es casi tan importante, quizás más, que el hecho de desarrollar una página web que a la vista de quien desee navegar en ella sea agradable y accesible; legalmente las empresas u organizaciones están obligadas a implementar mecanismos que cuiden, protejan y blinden los datos sensibles que determinado cliente debe registrar en sus páginas web con el deseo de adquirir un producto o servicio cualquiera; en Colombia y en el mundo se castiga la no seguridad en las páginas web y los diferentes delitos informáticos que a diario se cometen; se regula el comercio electrónico con el objetivo de garantizar a compradores y vendedores la seguridad de sus datos a través de la implementación de mecanismos de seguridad de la información.

Son 4 los mecanismos de seguridad de la información que se pueden implementar para dotar a la información de autenticidad e integridad; estos son:

1. Firmas digitales
2. Certificados digitales
3. Cifrado
4. SSL
5. Firewalls

Tabla 3. Mecanismos de seguridad de la información

Mecanismo	Descripción	Características	Ventajas
Firmas digitales	Es un conjunto de datos en forma electrónica, asociados a otros que pueden ser utilizados como medio de identificación del firmante. [46]	• Identifica de forma inequívoca al firmante. • Asegura la integridad del documento firmado. • Garantiza el no repudio.	• Facilita las operaciones que se desarrollan por medio de plataformas digitales. • Garantiza la autenticidad del documento. • Garantiza que el documento no ha sido modificado.

[46] CLINIC CLOUD. Contenidos digitales, firma digital. [Sitio web]. Bogotá D.C. [20.06.2021]. Disponible en: https://clinic-cloud.com/blog/firma-digital-definicion-como-funciona/

Certificados digitales	Es el único medio que permite garantizar técnica y legalmente la identidad de una persona en internet. Es un requisito obligatorio para que las instituciones puedan ofrecer servicios por internet.[47]	• Permite cifrar las firmas digitales. • Consta de una pareja de claves criptográficas, una pública y una privada.	• Da la garantía de que el documento no ha sido manipulado. • El firmante no podrá negar la autoría del documento. • Únicamente el destinatario puede abrir el documento.
Cifrado	Es un procedimiento de seguridad que consiste en alterar los datos que componen un archivo, de tal modo que se vuelvan ilegibles en caso de que sean interceptados por un tercero. [48]	• Criptografía simétrica: se usa en el uso de una única clave para cifrar y descifrar el documento. • Criptografía asimétrica: la clave debe ser enviada al receptor por medio de un canal digital.	• Evita el manejo inapropiado de la información. • Se minimiza el riesgo de manipulación y robo de la información. • Blinda las comunicaciones de una organización.
SSL	Es un estándar de seguridad que permite la trasferencia de datos cifrados entre un navegador y un servidor web. [49]	• Autentica la seguridad del sitio web. • Cifra la información transmitida.	• Garantiza a los usuarios que el sitio web que visitan es seguro. • Disminuye el riesgo de manipulación de la información.

[47] UPV. Universidad politécnica de Valencia. Área de sistemas de la información. [Sitio web]. Valencia, España. [20.06.21]. Disponible en: https://www.upv.es/contenidos/CD/info/711545normalc.html

[48] COLT. Beneficios del cifrado de datos para las empresas. [Sitio web]. España. [20.06.21.]. Disponible en: https://www.colt.net/es/resources/beneficios-del-cifrado-de-datos-para-las-empresas/

[49] VERISIGN. Certificados SSL. [Sitio web]. Lima. [20.06.21]. Disponible en: https://www.verisign.com/es_LA/website-presence/online/ssl-certificates/index.xhtml

Firewalls	Es un elemento informático que tata de bloquear el acceso a una red privada a personas que no han sido autorizadas. [50]	• Firewall de hardware: se halla instalado en el router que se usa para entrar a internet, protege los ordenadores de la red. • Firewall de software: viene con el sistema operativo del ordenador y solamente protege el equipo.	• Protege las redes informáticas de usuarios no autorizados. • Preserva la seguridad y privacidad de los navegantes.

Fuente: elaboración propia

Cada uno de los mecanismos listados y comparados anteriormente, tienen características, atributos, ventajas y desventajas diferentes, y la conjugación de 2 o más de estos asegurarán la seguridad total de los datos más sensibles tanto de vendedores como de compradores. Según expertos, el mecanismo de seguridad más usado son los firewalls, pues combina varios mecanismos de seguridad y esto genera que el nivel de confianza y seguridad de la información sea superlativo referente a los demás.

Sebastián Mollineti, español experto en seguridad informática, expresa que el 70% de las empresas, sin importar su actividad económica, implementan como mecanismo de seguridad en la información los llamados cortafuegos; los prefieren al garantizar la protección de datos que viajan en la red; además de la facilidad en su manipulación y uso. [51]

Aparte de los mecanismos mencionados anteriormente, es importante tener en cuenta los principios que buscan garantizar la seguridad en las transacciones, estos ya han sido referenciados anteriormente, pero es válido mencionarlos en este punto

[50] SOFTWARE LAB. Firewalls, todo sobre un firewall. [Sitio web]. España. [21.06.21]. Disponible en: https://softwarelab.org/es/que-es-un-firewall/

[51] MOLLINETI, Sebastián. Telefónica tech, mecanismos de seguridad. Blog empresarial. 2021.

donde se busca contextualizar más acerca de este tema en particular; dichos principios son:

- Principio de confidencialidad
- Principio de integridad
- Principio de accesibilidad

Tabla 4. Principios de seguridad

Principio	Descripción	Características
Principio de confidencialidad	Se refiere a los esfuerzos de una organización para mantener sus datos privados. [52]	• Controla el acceso a los datos para mantenerlos privados. • La clasificación de datos y controles de acceso disminuye el riesgo.
Principio de integridad	Indica que la información con la que se trabaja debe ser concisa y precisa, casi exacta. Tanto en el contenido como en los procedimientos involucrados.[53]	• Da la certeza de que la información no ha sido manipulada.
Principio de accesibilidad	Indica que la información debe estar disponible siempre que el usuario tenga que consultarla. [54]	• Permite al usuario el uso y consulta de la información cada vez que lo requiera. • Da la seguridad de que la información no ha sido modificada por terceros.

Fuente: elaboración propia

[52] MUNDOCONTACT. CIA, artículos web, seguridad informática. [Sitio web]. Lima. [21.06.21]. Disponible en: https://mundocontact.com/cia-los-tres-principios-fundamentales-de-la-seguridad-de-la-informacion/

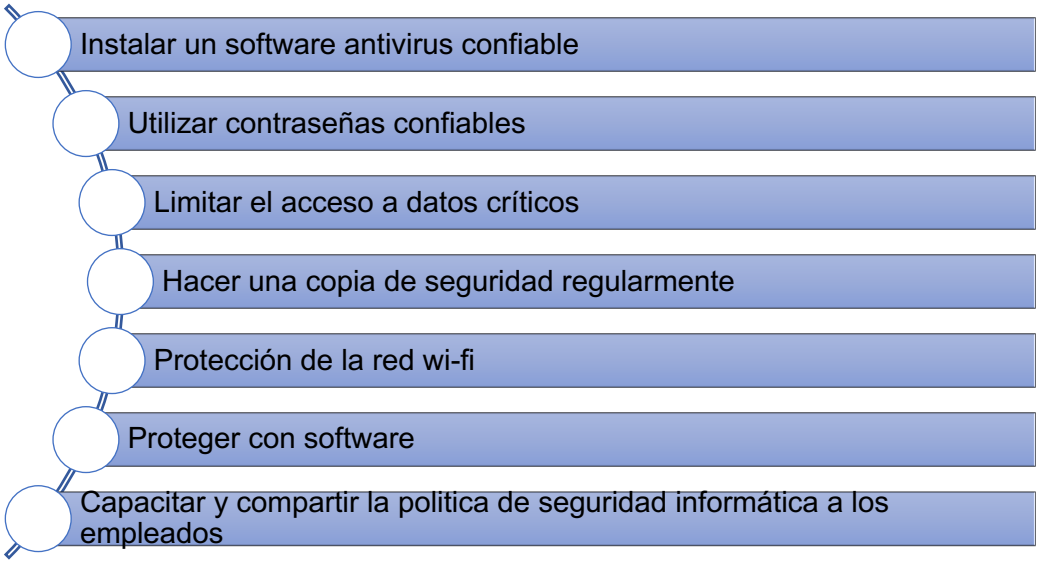
[53] UNIR. La universidad en la web. [Sitio web]. Bogotá D.C. [21.06.21]. Disponible en: https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/#:~:text=Proteger%20la%20informaci%C3%B3n%20significa%20garantizar,la%20disponibilidad%20de%20la%20informaci%C3%B3n.

[54] SGSI. Sistema de gestión de seguridad de la información. [Sitio web]. Bogotá D.C. [21.06.21]. Disponible en: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

También es importante mencionar algunos de los problemas de seguridad más comunes que pueden sufrir las transacciones electrónicas, entre estos se encuentran:

- **Código malicioso:** incluye una gran variedad de amenazas como virus, gusanos o troyanos.
- **Virus:** es un programa que tiene la capacidad para replicarse y extenderse a otros archivos.
- **Gusanos:** es un virus que está diseñado para propagarse entre máquinas.
- **Programas no deseados:** programas que son instalados en el computador sin la autorización de los usuarios.
- **Adware:** anuncios emergentes no deseados por el usuario.
- **Spyware**: programas que son usados para robar información.
- **Robo de identidad:** intentos engañosos para robar información confidencial.
- **Hackeo:** acciones que buscan dañar, desfigurar o interrumpir un sitio web.
- **Fraude de tarjeta de crédito:** uso de datos para robar información bajo el uso de identidad falsa.

A continuación, se puede observar la estrategia que los expertos sugieren a una empresa implementar con el fin de garantizar la seguridad en la información y/o datos que manejan. [55]



[55] ARATECNIA. Expertos en seguridad de la información, estrategias. [Sitio web]. México. [21.06.21]. Disponible en: https://aratecnia.es/medidas-de-seguridad-informatica/

DETERMINAR COMO ACTÚAN Y COMO SE DESARROLLAN LOS DIVERSOS SISTEMAS DE SEGURIDAD PARA TRANSACCIONES EN EL COMERCIO ELECTRÓNICO

Dentro de los mecanismos más importantes y efectivos para la seguridad en las transacciones electrónicas podemos encontrar:

1. Firmas digitales

En primer lugar, se debe definir que es una firma electrónica; entonces, es una técnica matemática utilizada con el fin de validar la autenticidad e integridad de un mensaje, un software o un documento digital.

A diferencia de una firma tradicional, manuscrita, la firma digital consta de dos claves o secuencias de caracteres separados. Este mecanismo consiste en aplicar mecanismos criptográficos al contenido de determinado mensaje o de un documento específico con el único objetivo de demostrar al receptor del mensaje los siguientes aspectos:

- ✓ Que el emisor del mensaje es real, es totalmente autentico **(autenticidad)**
- ✓ Que el emisor no puede negar que es él quien envía el mensaje **(no repudio)**
- ✓ Que el mensaje no ha sufrido alteraciones ni modificaciones desde el momento de su emisión **(integridad)** [56]

En Colombia bajo la Ley 527 de 1999, se reglamenta el acceso y uso de los mensajes de datos, firmas y comercio electrónicos, además de ello, se establecen las entidades encargadas de su certificación.[57]

La ley anteriormente mencionada establece que ambas partes pueden hacer uso de la firma electrónica si hay consentimiento mutuo en cualquiera de los acuerdos.

---

[56] ADOBE. Acrobat adobe. [Sitio web]. Bogotá D.C [21.06.21]. Disponible en: https://acrobat.adobe.com/la/es/sign/glossary/digital-signatures.html#:~:text=Las%20firmas%20digitales%20emplean%20ID,proveedores%20de%20servicios%20de%20confianza.

[57] COLOMBIA CONGRESO DE LA REPUBLICA. Ley 527 de 1999. (21, junio, 2021). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico. En: Presidencia de la república de Colombia. Bogotá D.C. 2021. 1P

En Colombia se reconocen dos tipos de firmas:

- ✓ **Firma digital:** tiene los mismos efectos y la misma fuerza que la firma manuscrita, de acuerdo con el Decreto 2364 de 2012, con mecanismos que garanticen autenticidad e integridad.
- ✓ **Firma electrónica:** Debe contar con los siguientes atributos para tener la misma validez que la firma manuscrita.
- ✓ Debe ser única a la persona que la usa.
- ✓ Es susceptible a su verificación.
- ✓ Esta bajo el control exclusivo de la persona que la usa.
- ✓ Está ligada a los mensajes o información, en caso de que la información cambie, la firma quedará inválida.
- ✓ Está ligada a la reglamentación estipulada por el gobierno nacional.

Es importante resaltar que la firma digital es totalmente legal y válida, y su único objetivo es cifrar los datos de determinado documento para proferirle mayor seguridad.

Funcionamiento

La firma digital basa su funcionamiento en la criptografía de una clave pública, que también se conoce como criptografía asimétrica. Hay tres algoritmos que conforman el proceso de una firma digital, veamos:

- ✓ Emisión de dos claves que están matemáticamente ligadas: un algoritmo genera una clave que debe ser siempre privada y única y de esta forma también se genera una clave pública que corresponde totalmente a la privada.
- ✓ Firma: en el momento en que el algoritmo reciba una clave privada e identifique el documento a firmar, se generará una firma.
- ✓ Verificación: dicho algoritmo debe comprobar que el mensaje es totalmente autentico, debe verificarlo en simultánea con la firma y la clave pública generada.

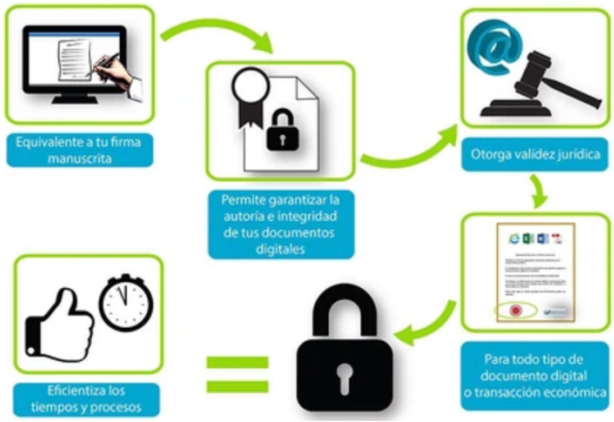
Dentro de todo el tema de la firma digital, es necesario conocer y manejar el llamado ***hash***, esto no es más que una serie de algoritmos que logran crear a partir de un texto, una contraseña o determinado archivo, una salida de números y letras, con el mismo tamaño siempre, que finalmente representa un resumen de toda la información que se le ha generado.

Cuando se desea crear una firma digital, el software crea un hash de una única dirección de los datos electrónicos que deben ser firmados. La clave privada se usa

para cifrar el llamado hash. Entonces, el hash ya cifrado y sumado a otra información adicional forman la firma digital.

En la siguiente imagen se detallan las características y beneficios de una firma digital.

Figura 12: Firma digital.



Fuente: https://ticsalborada1.fandom.com/es/wiki/18._Conductas_de_seguridad._Seguridad_activa:_Firma_digital_y_certificado_digital.

En caso de que el hash al momento de ser descifrado coincida con un segundo hash que fue calculado con los mismos datos, es la prueba de que los datos no ha sufrido ninguna modificación desde que se firmó. Si en dado caso los dos hashes NO coinciden, quiere decir que los datos se han alterado es decir que han perdido el atributo de la integridad, o por otro lado si la firma se ha creado con una clave privada que NO corresponde a la clave pública, indica que la firma carece de autenticidad.

Una de las ventajas de las firmas digitales que la persona que firmó no puede negar el hecho de haberlo realizado, atributo del no repudio; pues cabe resaltar que la firma digital es exclusiva tanto para el documento como para la persona que firma, es decir los relaciona. [58]

[58] GOB. Gobierno de España. AESA manejos electrónicos. [Sitio web]. España. [21.06.21]. Disponible en: https://sede.seguridadaerea.gob.es/SEDE_AESA/LANG_CASTELLANO/CONCEPTOS/QUE_FIRMA/#:~:text=El%20funcionamiento%20de%20la%20firma,p%C3%BAblica%20y%20una%20clave%20privada%3A&text=El%20emisor%20cifra%20el%20resumen,mediante%20la%20funci%C3%B3n%20%E2%80%9Chash%E2%80%9D.

Las firmas digitales cuentan con elemento que se denomina ***certificado digital***, este documento, contiene la firma y la vincula directamente con la identidad del firmante, esto verifica que la clave pertenece a una persona o entidad exclusiva y única.

Este mecanismo de seguridad se usa más que todo para proporcionar pruebas de autenticidad, no repudio e integridad de los datos a comunicaciones y transacciones realizadas a través de internet.

En conclusión, son tres las razones por las cuales un comercio que ofrezca sus productos y/o servicios por internet, debe implementar la firma digital:

- ✓ Asegura que los documentos son auténticos y provienen de una fuente que fue previamente verificada.
- ✓ El documento no ha sido víctima de alteraciones o modificaciones desde que fue firmado.
- ✓ Su identidad ha sido en primer lugar verificada por una organización totalmente confiable.

2. Criptografía

La criptografía es un arte y/o disciplina compleja que permite la protección de la información por medio del ocultamiento de esta. En el siglo pasado, la criptografía se usaba para ocultar y proteger información de militares o acerca de asuntos políticos.

Tipos de criptografía en la seguridad informática

- ✓ Criptografía simétrica: este tipo de criptografía tiene dos actores importantes: emisor y receptor. Esto quiere decir que los dos conocen la clave o la contraseña, pues previamente esta ha sido compartida por un canal sin seguridad o filtro alguno, por ejemplo, una llamada, un chat, un correo o por una carta.

Debido a la facilidad con la que se comparte la clave se genera una mayor vulnerabilidad, pues de la misma forma en cómo se transmite la contraseña así mismo se recibe, entonces es muy fácil interceptar el canal para romper el código y conocer la clave.

En la figura 13 se describen los actores y el proceso de cifrado con el método simétrico.

Figura 13: Criptografía simétrica.

Fuente: https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/

Una de las principales ventajas que ofrece la criptografía simétrica es la rapidez al momento de emitir y entregar los mensajes. Sin embargo, no es recomendable si el objetivo de la empresa es proteger y hacer privada la información.

- ✓ Criptografía asimétrica: este tipo de criptografía emplea dos claves, de esta forma se hace más robusto e impenetrable el mensaje. Una de estas claves es pública y no ofrece ningún tipo de protección, ya que el único objetivo que tiene es establecer un canal que sirva como medio para entregar el mensaje. La otra clave que conforma este tipo de criptografía es privada y tiene la responsabilidad de cifrar el mensaje para que este permanezca privado. Ambas claves son emitidas en el mismo momento y es el dueño el que tiene la potestad de decidir a quien desea revelárselas.

En la figura 14 se describen los actores y el proceso de cifrado con el método asimétrico.

Figura 14: Criptografía asimétrica.

Fuente: https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/

El código de cifrado tiene un tamaño aproximado de 2048 bits, por esto su gran robustez y el tamaño del código de cifrado; cada bit hace más difícil romper el código.

La desventaja que este mecanismo de seguridad ofrece es la lentitud a la hora de verificar los datos.

- ✓ Criptografía híbrida: es una combinación de los mecanismos anteriores y minimiza las desventajas a niveles tolerables.

La siguiente figura describe los actos (emisor y receptor) y un proceso de cifrado en el que se tienen propiedades del método simétrico y asimétrico

Figura 15: Criptografía Híbrida.

Fuente: https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/

Tabla 5. Tipos de criptografía

Tipo de criptografía	Descripción	Características
Criptografía simétrica	Este tipo de criptografía solo utiliza una clave para descifrar y cifrar el mensaje. Previamente se debe conocer el emisor y receptor, este es su punto débil, ya que se conoce la clave y puede ser objeto de interceptación. [59]	• Su objetivo es diseñar, implementar y hacer uso de sistemas criptográficos. • Ambas partes tienen acceso a la clave. • El cifrado simétrico es rápido. • No se ajusta a las firmas digitales.
Criptografía asimétrica	Permite establecer una conexión segura entre dos partes, autentificando mutuamente las partes y permitiendo el traspaso de información entre los dos.[60]	• Usa dos llaves para descifrar el mensaje: una llave pública y otra privada. • Para cifrar se usa la llave pública. • Para descifrar se usa la clave privada. • Las llaves son generadas por cada uno de los usuarios.
Criptografía hibrida	Es un método criptográfico que combina la criptografía asimétrica y simétrica. [61]	• Utiliza el cifrado de clave pública para compartir una clave para el cifrado simétrico. • No es tan fuerte que el cifrado simétrico. • La parte más débil es el hecho de tener que compartir la clave a ambas partes.

Fuente: elaboración propia

[59] GENBETA. Programadores web, criptografía. [Sitio web]. Colombia. [21.06.21]. Disponible en: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

[60] ALTAVOZ. Seguridad, cifrado. Tipos de cifrado. [Sitio web]. Valencia. [21.06.21]. Disponible en: https://www.altavoz.net/altavoz/blog/desarrollo/que-es-la-criptografia-asimetrica-y-por-que-es-importante

[61] BLOG. Criptografía. Blog. Bogotá D, C: 2017. [Consultado, 21.06.21]. Disponible en: https://criptografia.blogia.com/2008/052501-tipos-de-criptograf-a-h-brida.php

Resultado: teniendo en cuenta la comparación realizada, el tipo de criptografía más eficaz y seguro es la criptografía asimétrica, pues usa dos claves, una para cifrar y otra para descifrar; estas claves o llaves no debe ser compartidas entre las partes y cada una de esas establece la clave que desee.

- ✓ RSA: es un algoritmo de cifrado asimétrico o de claves públicas y es uno de los algoritmos más populares, eficaces y usados en la actualidad. Actualmente la mayoría de los sitios se desarrollan sobre SSL y únicamente permiten la autenticación a través de un cifrado asimétrico que esté basado en RSA.

  Esta técnica permite cifrar y descifrar información, por esta razón genera servicios de autenticidad e integridad, por ello se conoce como infraestructura de clave pública.

  Tal mecanismo, trabaja con dos claves, una es pública y la otra es privada; todo el contenido que no esté cifrado y que haya sido hecho con la clave pública será descifrado con la clave privada y viceversa del mismo modo.

  El cifrado de datos cobra gran importancia y relevancia a la hora de garantizar la seguridad de la información y la privacidad de estos; si la información llega a una persona no autorizada y esta intenta abrirla, solamente verá un grupo de letras y números que seguramente no entenderá.

3. Certificados digitales

El certificado digital va ligado directamente a la firma digital; es el único medio que garantiza de manera técnica y legal la identidad de una persona en la web. El certificado es un requisito indispensable para todas aquellas empresas u organizaciones que desean ofrecer sus productos o servicios por internet.

A su vez, el certificado digital permite la colocación de las firmas electrónicas en los documentos; la persona que recibe el documento firmado puede tener la certeza de que este es totalmente seguro y de que no ha sufrido ninguna alteración o modificación en su contenido y además el autor no podrá negar que fue él quien firmó el documento; por otro lado, el certificado digital permite cifrar el documento, lo que indica que solamente el destinatario puede tener acceso al documento. La principal ventaja de estos mecanismos es el ahorro del tiempo que significa tener un certificado digital, además del ahorro de dinero, pues puede realizar trámites administrativos por internet sin importar el día o la hora.

Funcionamiento

Un certificado digital se compone de dos claves criptográficas, una de estas es pública y la otra es privada; son creadas con un algoritmo matemático del tal modo que lo que se cifra por medio de una de las claves solo podrá ser descifrado con su clave pareja.

El titular de este certificado debe mantener bajo su dominio y de forma confidencial la clave privada, pues si de algún modo esta llega a ser robada, el delincuente podría sustituir al titular en la web; en caso de que eso pase, el titular deberá hacer la revocación del certificado lo más pronto posible, de la misma forma en que se bloquea una tarjeta cuando es robada o perdida.[62]

4. SSL (SECURE SOCKETS LAYER)

Es una tecnología estandarizada que tiene como objetivo cifrar los datos que viajan entre un navegador web y una página web, siempre manteniendo y asegurando la protección y seguridad de la conexión. Lo anterior, impide que un hacker pueda visualizar o modificar la información que está siendo transmitida de un lado a otro y de esta forma pueda incluir datos personales o financieros que no corresponden al mensaje que se envía.

Cabe resaltar que el SSL establece las comunicaciones seguras a través de certificados digitales.

Lo que hace el SSL es cifrar los datos que se trasfieren entre usuarios y páginas web, de tal forma que estos sean imposibles de leer a través del uso de algoritmos de cifrado que codifican los datos que son trasmitidos, impidiendo que los hackers puedan leerlos. La información que viaja a través de estos canales y que será cifrada con el SSL, puede ser cualquier dato confidencial o personal, como números de tarjetas de crédito, datos financieros, direcciones o nombres. Su versión actualizada es el TSL. [63]

---

[62] ING. En naranja. Certificados digitales, todo sobre certificados digitales. [Sitio web]. Colombia. [21.06.21]. Disponible en: https://www.ennaranja.com/economia-facil/certificado-digital/#:~:text=El%20certificado%20digital%20es%20un,reconocida%20como%20autoridad%20de%20certificaci%C3%B3n.

[63] GLOBALSIGN. Protocolos de cifrado. [Sitio web]. Brasil. [21.06.21]. Disponible en: https://www.globalsign.com/es/ssl-information-center/what-is-ssl

Funcionamiento

La siguiente figura muestra el uso de protocolo SSL en una página web

Figura 16: Uso del protocolo SSL.

Fuente: https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

La figura 17 demuestra que el SSL funciona de manera transparente frente al usuario, cuando se intenta acceder a un sitio web que es seguro, pasa lo siguiente:

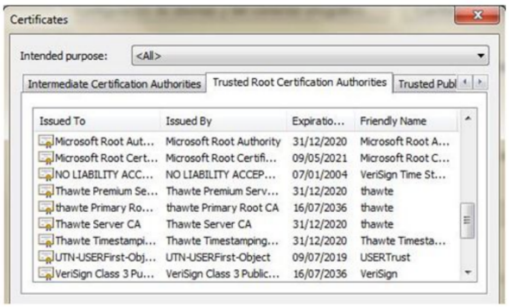
Figura 17: Funcionamiento general del SSL.

Fuente: https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

El navegador debe tener certeza del certificado del sitio web y debe realizar validaciones para confiar en el sitio; se debe validar que el certificado sea integro, que esté vigente y la originalidad del emisor.

La figura presentada a continuación es una ilustración de como se ven los certificados de seguridad instalados.

Figura 18: Validación de certificados.



Fuente https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

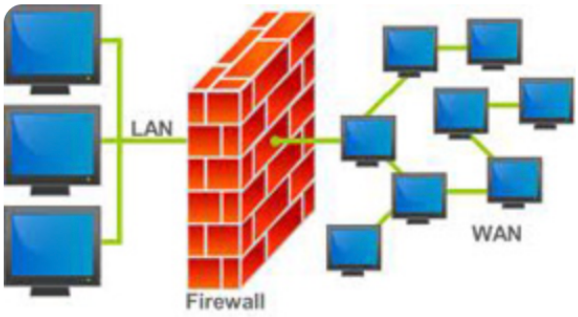
En conclusión, los comercios deciden usar el SSL porque este protege a gran escala los nombres de usuario, así como sus contraseñas, del mismo modo los formularios que suelen usarse en páginas web para enviar datos personales, imágenes o algún documento.

5. Firewalls

Este mecanismo es de carácter preventivo contra los ataques, realiza una inspección de los datos que entran y salen por determinado canal. Lo anterior impide que ciertos servicios y dispositivos que no estén autorizados accedan a la información que se busca proteger.

La figura 19 detalla el funcionamiento básico de un firewall.

Figura 19: Funcionamiento del Firewall.



Fuente: https://culturacion.com/cual-es-la-utilidad-de-un-firewall/

El software pude darse por medio de Software o de Hardware o a través de combinaciones de estos dos.

Los cortafuegos, son usados con frecuencia para evitar que usuarios de internet que no estén autorizados tengan acceso a redes que son privadas y que están conectadas a internet, especialmente las llamadas intranets.

La totalidad de los mensajes que puedan ingresar o salir de la intranet deben pasar por el cortafuegos, este examina minuciosamente cada mensaje y bloquea de inmediato todos aquellos que no cumplan con ciertos criterios de seguridad que ya han sido especificados. También es posible que el cortafuegos sea conectado a una tercera red que se llama Zona desmilitarizada o DMZ, allí están ubicados todos aquellos servidores de la organización o empresa que deben siempre permanecer accesibles desde una de las redes exteriores.

Cuando un cortafuegos está correctamente configurado, añade toda la protección necesaria a la red, pero es importante resaltar que en ningún caso puede considerarse que esta seguridad es suficiente, siempre debe buscarse que sea más segura cada día. La seguridad de la información debe abarcar ámbitos y niveles de trabajo y protección cada vez más altos y eficientes.
La función principal del cortafuegos es supervisar absolutamente todo el tráfico de datos de una red y validar si tiene permisos y de este modo bloquear toda la información que sea no deseada. [64]

[64] CISCO. Líder en firewalls, todo sobre cortafuegos. [Sitio web]. México. [21.06.21]. Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-

Tipos de Firewall

- ✓ Firewall de cliente: es un software que habita y permanece siempre en el propio equipo y que supervisa y valida todo el tráfico que de red que viaja en esta máquina.
- ✓ Equipo de Firewall: esto es un dispositivo físico que está conectado entre la internet y el equipo.

Ambos tipos de Firewall pueden bloquear el acceso que no sea deseado a tal equipo. Si bien un antivirus es muy importante, el Firewall es un complemento a este que puede dejar sin acción a un posible hacker.
El siguiente cuadro, permite al lector establecer de manera más fácil las diferencias entre cada uno de los mecanismos de seguridad y su funcionamiento; de este modo se podrá establecer cual es más seguro y viable a la hora de establecer estrategias de seguridad dentro de una organización.

Tabla 6. sistemas de seguridad

Sistema de seguridad	Descripción	Funcionamiento
Firma digital	Es una técnica matemática utilizada con el fin de validar la autenticidad e integridad de un mensaje, un software o un documento digital.	1. Emisión de dos claves. 2. Una vez se emitan las claves se procede con la firma del documento. 3. Se verifica la autenticidad del mensaje
Cifrado	Es un arte y/o disciplina compleja que permite la protección de la información por medio del ocultamiento de esta. Se clasifica en criptografía simétrica, asimétrica e hibrida.	1. Al darle clic a “firmar” se genera una huella digital única para ese documento, cualquier cambio emite un hash diferente. 2. El hash se cifra y la llave pública es combinada en una firma digital que se agrega al documento.

firewall.html#:~:text=Un%20firewall%20es%20un%20dispositivo,durante%20m%C3%A1s%20de%2025%20a%C3%B1os.

		3. El documento firmado está listo para ser distribuido.
Certificados digitales	Es el único medio que garantiza de manera técnica y legal la identidad de una persona en la web.	1. Se emiten dos claves, una privada y una pública. 2. Se crea un algoritmo matemático. 3. El documento puede ser firmado. 4. Se emite el certificado que asegura la autenticidad de documento.
SSL	Es una tecnología estandarizada que tiene como objetivo cifrar los datos que viajan entre un navegador web y una página web, siempre manteniendo y asegurando la protección y seguridad de la conexión	1. Se establece una conexión segura por SSL. 2. Presentación del certificado. 3. Transmisión de una clave de cifrado única. 4. Descifrado de la clave usando la clave privada.
Firewalls	Mecanismo de seguridad que realiza una inspección de los datos que entran y salen por determinado canal.	1. Funciona como una barrera entre internet u otras redes públicas y el computador. 2. El firewall debe: autorizar conexiones, bloquear conexiones y redireccionar un pedido de conexión sin avisar.

Fuente: elaboración propia

ESTABLECER LA IMPORTANCIA QUE TIENEN LOS SISTEMAS DE SEGURIDAD EN EL COMERCIO ELECTRÓNICO SUPONE PARA LA OPERACIÓN Y DESARROLLO DE UNA EMPRESA Y/O ORGANIZACIÓN.

Teniendo en cuenta el desarrollo de los objetivos anteriores y el análisis hecho a lo largo del presente trabajo, tomando en cuenta temas relevantes, como el escenario laboral en el que se desenvuelve el autor de este documento, que fue un impulso para tomar como objeto de estudio este tema, y un eje para desarrollarlo, pues a diario con las tareas que ejecuta, ve y entiende la responsabilidad que adquiere un comercio cuando decide incursionar en el tema del comercio electrónico en cuanto a la seguridad de sus clientes o usuarios, escenarios de la vida real en cuanto a la cantidad alarmante de fraudes que se realizan sobre las diversas plataformas web, puedo decir con certeza que todos y cada uno de los sistemas de seguridad que fueron identificados, analizados y estudiados en este documentos tienen un objetivo y ventajas diferentes entre sí, lo que indica que la combinación de dos o más de estos garantizaría mayor seguridad dentro de las transacciones electrónicas.

La implementación de estos mecanismos en las diferentes plataformas web que existen en internet y que permiten la realización de pagos, compras y ventas, que incluyen la manipulación de datos sensibles, son vitales y trascendentales a la hora ofrecer un servicio; una empresa que está dentro del comercio electrónico debe regirse por las leyes que se han implementado acerca de este tema, como la Ley de Comercio Electrónico en Colombia y demás decretos explicados en el marco legal de este documento.

La seguridad de la información no solo “asegura” los datos que reposan en la web, también juegan un papel fundamental en la parte organizacional de la empresa, pues una implementación correcta de mecanismos que garanticen seguridad va a generar como efecto inmediato una repercusión positiva en sus clientes, esto a la vez el crecimiento de la empresa en ventas o acciones y del mismo modo aumento en sus ingresos.

La empresa debe velar por la seguridad de los datos sensibles de sus clientes; por otro lado, las leyes reguladoras también protegen al comerciante, las plataformas de pago protegen el producto y el dinero en el efecto de la transacción.

A continuación, el lector podrá conocer algunos casos de éxito en empresas que han implementado mecanismos de seguridad de la información para el desarrollo de su actividad principal, lo cual busca demostrar la importancia que tienen dichos

mecanismos a la hora de innovar dentro del amplio mercado que supone el comercio electrónico en Colombia.

1. **Redeban Multicolor – pago facial:** la empresa de transacciones electrónicas Redeban y la cadena de supermercados Carulla, se aliaron para poner en marcha el primer sistema del país que permite pagos por medio de reconocimiento facial.

   Este mecanismo funciona escaneando el rostro en la aplicación que fue desarrollada, posteriormente se vincula con la tarjeta financiera y se finalmente el cliente se acerca a cualquiera de los puntos de pago habilitados para esta modalidad.

   Este modo de pago, está dotado de altos estándares de seguridad que garantizan al usuario la integridad y confidencialidad de sus datos personales.

   Según las directivas de Redeban, se estima que para el 2024 este mecanismo genere ingresos por US$7,000 millones, con un crecimiento del 16% anual. [65]

2. **Credibanco y Visa – transferencias persona a persona:** la empresa de pagos electrónicos Credibanco y la multinacional Visa, anunciaron el lanzamiento de transferencias en línea con tarjetas a través de una aplicación llamada “PaGo”; aplicación que se ha convertido en la primera app móvil de transferencia de dinero nacionales en tiempo real.

   Este mecanismo, busca habilitar las transferencias en tiempo real sin necesidad de intercambiar números de cuenta o pasar por oficinas de manera presencial.

   De acuerdo con declaraciones dadas por el gerente de Credibanco, Humberto Guihur, este servicio está certificado con altos estándares de seguridad y asegura que las plataformas están blindadas de tal modo que

[65] LR. La República, actualidad financiera en Colombia. Bancos. Redeban desarrolla un servicio de pago facial en alianza con Carulla en Colombia. [Sitio web]. Bogotá D.C. [21.06.21]. Disponible en: https://www.larepublica.co/finanzas/redeban-desarrolla-servicio-de-pago-facial-en-colombia-en-alianza-con-carulla-2961316

garanticen la seguridad ante ataques cibernéticos; es un servicio totalmente gratuito que busca generar ganancias por almeno US$8.000 millones para ambas empresas. [66]

3. **BOLD – link de pagos:** la reconocida empresa de datafonos BOLD, implementó el denominado link de pagos, con el fin de facilitar al usuario la compra de bienes y servicios por medio de su plataforma, si tener que usar las tarjetas físicamente. Este mecanismo de pago está certificado con el estándar PCI DSS nivel 1 (corresponde a negocios que manejen más de 6 millones de transacciones por tarjetas Visa o MasterCard al año)[67], para garantizar al usuario que los datos suministrados están seguros y no serán alterados. [68]

Los anteriores son los casos de éxito que se han implementado en grandes empresas colombianas cuya actividad económica está dedicada al comercio electrónico; cada uno de estos proyectos han sido puestos en marcha implementando altos y robustos mecanismos de seguridad en la información que los usuarios suministran en las diferentes plataformas de pago electrónicas existentes.

[66] LR. La República, actualidad financiera en Colombia. Bancos. Credibanco y Visa lanzaron el primer servicio de transferencias persona a persona en Colombia. [Sitio web]. Bogotá D.C. [21.06.21]. Disponible en: https://www.larepublica.co/finanzas/credibanco-y-visa-lanzaron-el-primer-servicio-de-transferencias-persona-a-persona-3162090

[67] QUALITYTELECOM. Riesgos de seguridad en pagos con tarjeta. [Sitio web]. Bogotá D.C. [21.06.21]. Disponible en: https://qualitytelecom.es/que-es-certificacion-pci-dss-nivel-1/#:~:text=%E2%80%93%20El%20PCI%2DDSS%20Nivel%201,Visa%20o%20Mastercard%20cada%20a%C3%B1o.

[68] BOLD. Datafonos. [Sitio web]. Bogotá D.C. [21.06.21]. Disponible en: https://bold.co/

CONCLUSION

La seguridad de la información juega un papel fundamental en el desarrollo y ejercicio de la actividad económica de una empresa, no se puede desarrollar una página web sin contemplar el hecho de hacerla segura para quienes van a navegar en ella, así mismo para quienes recibirán ingresos a través de ese sitio web.

Por todo lo analizado anteriormente, se concluye este documento afirmando que la seguridad de la información es uno de los temas más importantes que debe ser tratado dentro de un comercio u organización que ponga a la venta sus productos o que ofrezca sus servicios a través de internet.

Todos los mecanismos que existen actualmente para asegurar la información sensible de los usuarios son efectivos si se implementan de manera correcta, lo ideal es combinarlos y usar más de uno para garantizar un nivel más alto de seguridad.

Es importante resaltar que el propietario de la plataforma no debe confiarse del nivel de seguridad que ofrece, siempre debe prever y actuar para que cada día se más segura su plataforma, consultando expertos en el tema.

Por otro lado, es importante que el consumidor conozca sus derechos y deberes a la hora de adquirir productos o servicios en la web, debe tener claras las leyes que lo protegen y de este modo su experiencia será siempre positiva.

RECOMENDACIONES

Una vez concluida la presente monografía y en base a los resultados recogidos luego de la investigación, así como al aporte bibliográfico de este texto monográfico, se pone a consideración del lector y de la comunidad educativa que tenga acceso al mismo, investigar sobre otros aspectos relacionados con la seguridad en la información y en transacciones electrónicas, mecanismos para prevenir robos de información sensible; revisar más a fondo casos de éxito sobre empresas u organizaciones que hayan implementado mecanismos para prevenir ataques e incrementar la seguridad en sus diversas plataformas.

A continuación, dejo algunas recomendaciones que pueden ayudar al lector:

- Extender los estudios expuestos en la monografía en base a la seguridad en la información.
- Analizar con mayor detenimiento casos de éxito donde se hayan desarrollado y aplicado mecanismos de seguridad.
- Incluir y tener en cuenta opiniones de expertos que permitan ampliar el conocimiento acerca del tema tratado.
- Realizar un estudio sistemático y amplio sobre la seguridad en transacciones electrónicas en países del primer mundo.
- Revisar periódicamente las nuevas técnicas que las empresas u organizaciones diseñan e implementan con el fin de blindar las transacciones electrónicas en el mundo actual.

WEBGRAFÍA

ALFERDO, a. e, “SSL, SET y otros protocolos de seguridad” Internet: (https://www.ecommerce-nation.es/ssl-set-y-otros-protocolos-de-seguridad-en-ecommerce/)

ASTAÑEDA AYALA, maría juliana, “seguridad en las transacciones electrónicas”. Internet: (https://www.javeriana.edu.co/biblos/tesis/derecho/dere6/DEFINITIVA/TESIS22.pdf)

CARDENAS, Alfredo, “Ventajas y desventajas de los diferentes métodos de pago”. Internet: (https://quaderno.io/es/blog/ventajas-y-desventajas-de-los-diferentes-metodos-de-pago/)

CARVAJAL, Á, “Seguridad Ecommerce: los 4 ciber ataques más comunes y cómo mitigarlos”. Internet: (https://www.swhosting.com/blog/seguridad-ecommerce-los-4-ataques-mas-comunes/)

CEUPE, e. b, “La seguridad en las transacciones comerciales electrónicas”. Internet: (https://www.ceupe.com/blog/la-seguridad-en-las-transacciones- comerciales-electronicas.html)

COMERCIO, S, “¿Cómo va el comercio electrónico en Colombia?”. Internet: (ttps://digisap.com/va-comercio-electronico-colombia/)

“¿Cómo funcionan las Firmas Digitales?”. Internet: (https://www.globalsign.com/es/blog/como-funcionan-las-firmas-digitales/)

“¿Cuáles son las ventajas y desventajas del eCommerce?”. Internet: (https://www.actualidadecommerce.com/cuales-las-ventajas-desventajas-del-ecommerce)

DINERO, “E-commerce en Colombia va por buen camino”. Internet: (https://www.dinero.com/tecnologia/articulo/asi-avanza-el-comercio-electronico-en-colombia/275169)

EDITORS, “Análisis y evaluación de riesgos de seguridad de la información: identificación de amenazas, consecuencias y criticidad”. Internet: (https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/)

ESET Latinoamérica, “Seguridad en las transacciones comerciales en línea” Internet: (https://www.academiaeset.com/default/store/158508-seguridad-en-las-transacciones-comerciales-en-linea)

“Evolución de la innovación en pagos electrónicos a través de la historia, E. H. (s.f.). Evolución de la innovación en pagos electrónicos a través de la historia”. Internet: (https://newsroom.mastercard.com/latin-america/es/photos/evolucion-de-la-innovacion-en-pagos-electronicos-traves-de-la-historia/)

EXPERTOS, e, “¿Qué es la seguridad informática y cómo puede ayudarme?”. Internet: (https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/)

GUEDEZ, A, “Criptografía y seguridad informática: El ciclo de vida de claves y contraseñas y su relación con tus entornos digitales”. Internet: (https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/)

GUTIÉRREZ AMAYA, Camilo, “7 consejos para realizar transacciones seguras” Internet: (https://www.welivesecurity.com/la-es/2012/06/27/transacciones-seguras-internet/)

“Herramientas que facilitan las transacciones de eCommerce – Observatorio”. Internet: (https://www.observatorioecommerce.com.co/herramientas-facilitan-transacciones)

“Historia del datafono en Colombia”. Internet: (https://www.credibanco.com/sobre-credibanco)

IBM, Knowledge Center. Internet: (https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/bd34064_.htm)

“La seguridad en el comercio electrónico”. Internet: (https://www.webscolar.com/la-seguridad-en-el-comercio-electronico)

“La seguridad en las transacciones - Portal del comerciante”, Internet: (https://www.portaldelcomerciante.com/es/articulo/la-seguridad-transacciones)

“La seguridad en las transacciones - Portal del comerciante”. Internet: (https://www.portaldelcomerciante.com/es/articulo/la-seguridad-transacciones)

LENA ACEBO, Francisco Javier, “Nuevos métodos de pago online, seguridad y confiabilidad”. Internet: (https://repositorio.unican.es/xmlui/handle/10902/7884)

LOPEZ, Luis, “Sistemas de pago seguro. Seguridad en el comercio electrónico”. Internet: (https://dialnet.unirioja.es/servlet/articulo?codigo=3039867)

MADDEN, M, “¿QUÉ SON SSL, TLS Y HTTPS...?”. Internet: (https://www.digicert.com/es/what-is-ssl-tls-https/)

MARTINEZ, M. R. *Nuevos métodos de pago online, seguridad y confiabilidad.* España. 2015

MEDINA, J, “¿Qué es una firma digital?”. Internet: (https://blog.signaturit.com/es/que-es-una-firma-digital)

MINTIC, m. t, “Seguridad en el comercio electrónico”. Internet: (https://www.mintic.gov.co/portal/inicio/Micrositios/Soy-ciberseguro/Consejos/18773:Seguridad-en-el-comercio-electronico-Banca-en-linea)

MOLINA, C, “Seguridad informática y comercio electrónico”. Internet: (https://issuu.com/camilomolina99/docs/seguridad_informatica_y__comercio_e)

OROPEZA, D, “La competencia económica en el comercio electrónico y su protección en el sistema jurídico mexicano. En La competencia económica en el comercio electrónico”. Internet: (https://archivos.juridicas.unam.mx/www/bjv/libros/10/4667/4.pdf)

P, “Seguridad en comercio electrónico, métodos de pago seguros”. Internet: (https://portaley.com/2013/10/seguridad-en-comercio-electronico-metodos-de-pago-seguros/)

REDACCION EL TIEMPO, “Casi todo sobre el comercio electrónico” Internet: (https://www.eltiempo.com/archivo/documento/MAM-915340)

REYES, H. (s. f.), “Mecanismos Seguridad en Comercio Electrónico”. Internet: (https://prezi.com/q8gw5pzmlz8t/mecanismos-seguridad-en-comercio-Electronico)

SANCHEZ, Adriana, “¿Qué son SSL, TLS y HTTPS?”. Internet: (https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https)

SANDOVAL, A, “Firewall”. Internet: (http://leoecommerce.blogspot.com/p/blog-page_21.html)

SANDOVAL, Juan, “Seguridad de la Información”. Internet: (http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion)

"Seguridad en el Comercio Electrónico - Comercio electrónico". Internet: (https://sites.google.com/site/webcelectronico/-en-que-consiste-el-comercio-electronico/seguridad-en-el-comercio-electronico)

"SEGURIDAD EN EL COMERCIO ELECTRÓNICO". Internet: (https://www.cecarm.com/Guia_Seguridad_en_el_comercio_electronico_-_CECARM.pdf-6559)

"Seguridad en las transacciones digitales - Observatorio eCommerce". Internet: (https://www.observatorioecommerce.com.co/seguridad-en-las-transacciones-digitales/)

SEPULVEDA, Francisco, "Medios de pago electrónico". Internet: (https://www.portaldelcomerciante.com/es/articulo/medios-pago-electronico)

SEPULVEDA, Francisco, "Seguridad en el comercio electrónico". Internet: (http://www.vsantivirus.com/comercio-electronico.html)

SEPULVEDA, Fransisco, "EL CIFRADO WEB (SSL/TLS)". internet: (https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls)

SEPULVEDA, Fransisco, "Normas ISO sobre gestión de seguridad de la información". Internet: (http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html)

SIC GOV, s. g, "Comercio Electrónico en Colombia". Internet: (https://www.sic.gov.co/recursos_user/documentos/promocion_competencia/Estudios_Economicos/Estudios_Economicos/Estudios_Mercado_E-commerce.pdf)

SICE, "Comercio Electrónico/Legislación Nacional – Colombia" Internet: (http://www.sice.oas.org/e-comm/legislation/col2.asp)

"Todo Sobre ISO8583". Internet: (https://www.chileoffshore.com/es/interesting-articles/115-todo-sobre-iso8583)

TORO, R, "¿Qué significa la Seguridad de la Información?". Internet: (https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/)

UPV, "Que es un Certificado Digital?: Certificados Digitales". Internet: (https://www.upv.es/contenidos/CD/info/711545normalc.html)

V, s.f, “La historia del ecommerce en Colombia”. Internet: (https://www.vendesfacil.com/plataformas-empresariales/desde-cuando-en-colombia-comenzamos-a-adoptar-la-modalidad-de-comprar-en-internet/)

VENDESFACIL, v. f, “Mitos y verdades del comercio electrónico en Colombia” Internet: (https://www.vendesfacil.com/plataformas-empresariales/mitos-y-verdades-del-comercio-electronico-en-colombia/)

VILLAVECES, S, “¿Cómo es la ley de comercio electrónica en Colombia?”. Internet: (https://www.pymas.com.co/ideas-para-crecer/ecommerce/ley-comercio-electr%C3%B3nico)