IF-6201 INFORMÁTICA APLICADA A LOS NEGOCIOS II CICLO 2020

Trabajo de Investigación.

Profesor: Rolando Herrera Sanchez

Integrantes:

Karolina Montenegro Guzmán B64543

Jahanel Rivera Barboza B65875

Maikel Matamoros Zuñiga B64219

Tema: Seguridad en Negocios Electrónicos.

Tabla de contenidos

Introducción

A modo introductorio podemos decir, que la seguridad, es un aspecto clave para generar en las empresas y en los consumidores la confianza necesaria para que el comercio electrónico se desarrolle. La necesidad de generar confianza, en la que coinciden prácticamente todas las asociaciones de la industria, administraciones, etc. Es especialmente importante debido al hecho de que Internet es una red abierta y a la sensación de inseguridad que se genera entre los usuarios es muy fuerte.

Como es bien conocido, los medios de pago tradicionales sufren numerosos problemas de seguridad: falsificación de billetes, falsificación de firmas, cheques sin fondo, etc. Por otro lado, los medios de pago electrónicos, además de estar sujetos a los mismos problemas anteriores, presentan riesgos adicionales, pues a diferencia del papel, los documentos digitales pueden ser copiados perfectamente y cuantas veces se desee, las firmas digitales pueden ser falsificadas por cualquiera que conozca la clave privada del firmante, la identidad de una persona puede ser asociada de forma inequívoca con la información relacionada en cada pago, etc.

Es por ello que es necesario establecer nuevos mecanismos de seguridad para los nuevos medios de pago electrónicos, si se quiere que tanto las entidades bancarias como los usuarios finales acepten de forma generalizada estos nuevos medios de pago. Por otro lado, si los sistemas de pago electrónicos son bien diseñados, pueden proporcionar una mayor seguridad y flexibilidad de uso que la ofrecida por los medios de pago tradicionales

Dicho lo anterior, en este presente documento, vamos a explicar y mencionar, algunos sistemas de seguridad que utilizan las empresas para sus negocios, así también mencionar cuales son los protocolos de seguridad más importantes que se deben usar.

También, para nadie es un secreto, que existen bastantes riesgos, a los cuales estamos expuestos nosotros tanto como del lado de cliente, así como de lado técnico, es por eso, que en el transcurso de este presenta investigamos, vamos a mostrar a cuáles riesgos estamos expuestos, y también un caso de estudio donde se presentó un gran riesgo en una empresa hotelera y la cual no tomó reaccionó de la mejor manera.

Finalmente, explicaremos algunos consejos, y la importante que tiene este tema, tan controversial hoy en día, y del cual podamos ser precavidos con nuestros datos personales

Conceptos

¿Qué es la seguridad en el negocio electrónico?

La seguridad en el negocio o comercio electrónico y específicamente en las transacciones comerciales es un aspecto de suma importancia, esto porque es necesario disponer de un servidor seguro a través del cual toda la información confidencial es encriptada y viaja de forma segura.
Además de brindar confianza tanto a proveedores como compradores que hacen del comercio electrónico su forma habitual de negocios

Los sitios web de comercio electrónico tienen que tomar todas las medidas de seguridad necesarias para garantizar la protección de la información personal y financiera de sus clientes. Es por eso, que brindar un alto nivel de seguridad en los comercios electrónicos, cada día es fundamental, dado que tenemos información tan sensible tanto como los clientes, como para la empresa, que debemos protegerla dado que viaja por redes.

Niveles de Seguridad

¿Qué niveles de seguridad se deben considerar para pagos en plataformas comerciales?
Básicamente se trataría de garantizar cuatro principios.

1. **Principio de autenticidad**

   Cuando la persona o empresa que dice estar al otro lado de la red es quién dice ser.

2. **Principio de integridad**:

   Es lo transmitido a través de la red no haya sido modificado.

3. **Principio de intimidad**:

   Se da cuando los datos transmitidos no han sido vistos durante el trasiego telemático.

4. **Principio de no repudio**:

   Se da cuando lo transmitido no pueda ser repudiado o rechazado.

Maneras de mejorar la seguridad de tu tienda online y proteger los datos de tus clientes

1. Utiliza un administrador de contraseñas.

Este administrador va a generar fuertes contraseñas para los sitios que visites y las almacenará y encriptará en una especie de "caja fuerte" a la que podrás acceder con una contraseña maestra. Esto asegura que tus contraseñas no sólo serán indescifrables, también tendrás una para cada sitio que visites –una de las medidas más importantes y eficaces que puedes tomar en temas de seguridad.

Ejemplo de 2 aplicaciones que lo hacen:

A. Keepass
B. 1Password

Los navegadores web, por ejemplo Chrome, tiene su propio administrador de contraseñas, pero es muy riesgoso dado que

El mayor riesgo que presenta es que si un atacante tuviese acceso a la computadora podría obtener fácilmente las contraseñas, descifrarlas y robarlas en texto plano. Este tipo de comportamiento ha sido observado en múltiples códigos maliciosos e incluso en troyanos bancarios dirigidos específicamente a Latinoamérica, donde se pretende robar credenciales de acceso a sitios de banca en línea.

2. Encripta tu tienda online

Tradicionalmente, la mayoría de las tiendas online utilizan **certificados SSL** para **proteger la información personal que sus clientes** ingresan durante el proceso de compra. Si bien es cierto que tu proceso de compra está seguro, probablemente en el resto de tu tienda online aún utilizas el protocolo HTTPS. Esta ha sido una práctica bastante común durante los últimos 20 años.

3. Habilita la autenticación de dos pasos

Habilitar la autenticación de dos pasos (o dos factores) proporciona un nivel adicional de seguridad al exigir dos tipos de información por cada nuevo intento de inicio de sesión: el cliente recibirá la contraseña de su cuenta y un código de autenticación vía SMS o con una

aplicación. Esto asegura que incluso si alguien descubre tu contraseña, todavía necesitan acceso a tu dispositivo móvil para realizar un inicio de sesión exitoso.

4. Encripta tus dispositivos

Encriptar o cifrar tu información te permite que esté oculta para que no se pueda acceder a ella sin conocimientos especiales (como una contraseña). Cifrar tus dispositivos te asegurará que la información confidencial que tengas en ellos esté protegida, incluso si alguien trata de tener acceso de manera física.

Así es como esto se logra:

- Mac – utiliza FileVault para encriptar tu disco, directamente en tu panel de configuración.
- iPhone – puedes encriptarlo al habilitar la contraseña del dispositivo.
- Android – Selecciona la opción “Encriptar teléfono” en la sección de seguridad dentro de tu menú de configuración

5. Actualiza tu software.

Es cierto que encriptar tu información es importante, pero probablemente tu software también este vulnerable. La mejor manera de enfrentar la vulnerabilidad de tu software es asegurar que tu sistema operativo, navegador y software de computadora este actualizado, para evitar hacer clic en enlaces de descargas falsas que representen un riesgo para ti.

Estas son algunas maneras de facilitar este proceso:

- Desactiva las actualizaciones automáticas en Windows/OS X
- Cambia de navegador a Firefox o Chrome, dos navegadores que se actualizan automáticamente

- No ignores las actualizaciones de Java o Adobe –casi siempre contienen información importante en temas de seguridad
- Instala un software anti-malware como MalwareBytes

¿Por qué la seguridad es una necesidad en el comercio electrónico?

En la actualidad con el gran volumen de transacciones que se realizan por medio de internet, los comercios electrónicos son fuente de múltiples de esas transacciones, lo cual le da un peso extra a los dueños de los comercios electrónicos, a las empresa que usan este método para poder tener contacto con sus clientes y posicionar sus productos o servicios a disposición.

La seguridad para los compradores es tan importante como el mismo precio del producto. Es sumamente importante lograr interesar al público objetivo, recibir sus visitas, que se registren y seleccionen los productos, y los compren. Sin embargo, el éxito de la transacción involucra el hecho de que el usuario introduzca los datos de su tarjeta de crédito para concluir la compra.

No es de extrañar que existan personas que quieran sacar provecho de esto, básicamente los métodos de robo y estafa también han crecido y evolucionado a gran medida mientras más avanza la tecnología, por eso las empresas deben tomar muy en cuenta la necesidad de implementar todas las medidas posibles para protegerse ellos como negocio a la vez que también protegen a sus consumidores.

La implementación de las medidas necesarias para poder tener un nivel de seguridad óptimo no es algo simple, es un poco complicado y debe cumplir ciertos estándares, pero esto es de suma importancia para poder mantener el orden del negocios. López (2018) menciona una razón sumamente importante que todo negocio debe tomar en cuenta, este mismo menciona que “Cumplir con las medidas necesarias, permitirá que los compradores tengan más confianza en tu negocio”. Esto es una prioridad para las empresas, la confianza que tiene un cliente a la hora de realizar una compra es algo sumamente importante, están confiando en el negocio sus datos personales, datos que son sumamente valiosos y un negocio sin seguridad puede ser blanco fácil de ataques.

Cuando una empresa sufre ataques y pierde información de sus clientes, la credibilidad de esta se ve claramente manchada y puede sufrir pérdidas económicas increíblemente altas, lo cual es claramente una señal de alarma para evitar futuros inconvenientes.

Sistemas de Seguridad

Algunos sistemas de seguridad que se pueden implementar en sus negocios serían:

1. Encriptación
2. Firma Digital
3. Protocolo SET
4. Firmas Electrónicas
5. Certificados de Autenticidad
6. Criptografía
7. Hackers

1. **La encriptación** es el conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada. Con la encriptación la información transferida solo es accesible por las partes que intervienen (comprador, vendedor y sus dos bancos).

2. **La firma digital,** evita que la transacción sea alterada por terceras personas sin saberlo**. El certificado digital,** que es emitido por un tercero, garantiza la identidad de las partes**.**

3. **Protocolo SET**: Secure Electronic Transactions es un conjunto de especificaciones desarrolladas por VISA y MasterCard, con el apoyo y asistencia de GTE, IBM, Microsoft, Netscape, SAIC, Terisa y Verisign, que da paso a una forma segura de realizar transacciones electrónicas, en las que están involucrados: usuario final, comerciante, entidades financieras, administradoras de tarjetas y propietarios de marcas de tarjetas.

   SET constituye la respuesta a los muchos requerimientos de una estrategia de implantación del comercio electrónico en Internet, que satisface las necesidades de consumidores, comerciantes, instituciones financieras y administradoras de medios de pago.

   Por lo tanto, SET dirige sus procesos a:

   Proporcionar la autentificación necesaria.

Garantizar la confidencialidad de la información sensible.

Preservar la integridad de la información.

Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

4. **Firmas electrónicas:** las relaciones matemáticas entre la clave pública y la privada del algoritmo asimétrico utilizado para enviar un mensaje, se llama firma electrónica (digital signatures).

   Quien envía un mensaje, cifra su contenido con su clave privada y quien lo recibe, lo descifra con su clave pública, determinando así la autenticidad del origen del mensaje y garantizando que el envío de la firma electrónica es de quien dice serlo.

5. **Certificados de autenticidad**: como se ha visto la integridad de los datos y la autenticidad de quien envía los mensajes es garantizada por la firma electrónica, sin embargo existe la posibilidad de suplantar la identidad del emisor, alterando intencionalmente su clave pública. Para evitarlo, las claves públicas deben ser intercambiadas mediante canales seguros, a través de los certificados de autenticidad, emitidos por las Autoridades Certificadoras.

   Para el efecto SET utiliza dos grupos de claves asimétricas y cada una de las partes dispone de dos certificados de autenticidad, uno para el intercambio de claves simétricas y otro para los procesos de firma electrónica.

6. **Criptografía:** Es una aplicación técnica para cifrar datos (ocultar informaciones y conocimientos confidenciales) que se ha venido desarrollando mediante civilizaciones más antiguas, como el método que altera el orden de las letras a 3 espacios.

7. **Los Hackers:** Son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección. Su motivación abarca desde el espionaje industrial hasta el mero desafío personal. Internet, con sus grandes facilidades de conectividad, permite a un usuario experto intentar el acceso remoto a cualquier máquina conectada, de forma anónima. Las redes corporativas u ordenadores con datos

confidenciales no suelen estar conectadas a Internet; en el caso de que sea imprescindible esta conexión, se utilizan los llamados cortafuegos, un ordenador situado entre las computadoras de una red corporativa e Internet. El cortafuegos impide a los usuarios no autorizados acceder a los ordenadores de una red, y garantiza que la información recibida de una fuente externa no contenga virus.

Seguridad en las transacciones y los medios de pago. Protocolos de seguridad

¿Qué sistemas de seguridad existen hoy en día para el comercio electrónico?

Para asegurar las transacciones en línea, fundamentalmente se utilizan 2 protocolos se seguridad: el SSL y SEL
El SSL (Secure Sockets Layer) es un protocolo de intercambio de información que permite asegurar la autenticación, confidencialidad e integridad de los datos que se transmiten a través de internet
El SET (Secure Electronic Transaction) es un conjunto de especificaciones de seguridad desarrollado por Visa y MasterCard, junto con empresas líderes en tecnología, que asegura la confidencialidad e integridad de la información transmitida.

Consejos para tu comercio electrónico

Consejos para mantener y transmitir la seguridad en tu negocio

1) Ofrecer información clara y concisa sobre los productos y sus condiciones.
2) Usar un servidor seguro para alojar las páginas del comercio.
3) Añadir políticas de seguridad al servidor del comercio para aumentar la confianza de los clientes en las compras.
4) Cuidar la privacidad de los datos del cliente. Solicitar sólo los datos necesarios.
5) Aportar a los clientes información sobre la política de privacidad de la empresa.
6) Ofrecer varias alternativas de pago.

Principales riesgos del negocio e-commerce

¿A qué riesgos estoy expuesto al conectarme a internet?

1. Se crean vías de acceso para los miles de virus que se encuentran en la red.

2. Cuando un virus penetra un sistema puede afectar todos los archivos de las unidades de disco duros y programas en general, dañando y afectando su funcionamiento, lo que genera pérdida de tiempo, de dinero y en el peor de los casos el daño total del equipo.

3. La información que se almacena en el computador, también se ve expuesta y puede llegar a ser conocida, borrada o modificada.

4. Para una empresa puede significar la pérdida de reputación, miles o millones de pesos, o la parálisis de actividades, pérdida de información reservada, etc. 45 Sistema operativo utilizado para la interconexión de redes.

También hay atacantes internos y externos:

Los ataques internos son aquellos que se encuentran dentro de la misma empresa - empleados directos (empleados). Estos son difíciles de prevenir, depende de la lealtad y confianza que tengan entre el empleador y trabajador y los externos tienden a ser más peligrosos, pero menos frecuentes aquí es donde depende el nivel de seguridad que tenga la empresa para su comercio.

Existen personas fraudulentas que desean obtener ganancias a través del daño hacia los sistemas y los usuarios, esto cada vez se ha visto más creciente ha generado que las empresas tomen medidas más drásticas para protegerse a ellos mismo y a los cliente que realizan sus compras en sus comercios. Algunos de los peligros o riesgos que se corren son los siguientes:

Phishing

En la actualidad uno de los métodos más comunes de escuchar es el Phishing. Esta técnica es muy utilizada debido a la facilidad que se puede llevar a cabo y básicamente los mismos usuarios son los que se encargan de hacer todo el trabajo. Beneitez et al.(s.f.) hacen referencia a esta técnica y lo definen como "Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta". Como se puede ver el objetivo principal es poder conseguir la información sensible de los clientes. Para esto hacen uso del engaño

mediante correos o mensajes que parecen reales que normalmente tienen como objetivo que se ingrese a ellos y haga ciertas acciones que se ven normales , pero al final van a dejar la información expuesta.

Defacement

Otro de los posibles peligros es el denominado Defacement. El Defacement es un método de ataque contra una empresa muy peligroso debido a que es difícil de localizar a simple vista y se aprovecha de la credibilidad de la empresa así como de la fidelidad de los mismos clientes. Beneitez et al.(s.f) menciona que este proceso consiste básicamente en modificar de manera parcial o total una página web. Este método tiene múltiples factores los cuales motivan su ejecución, pero normalmente se hace con el fin de dañar la imagen de la empresa o conseguir información personal de los usuarios mediante acciones modificadas en la página web víctima.

SQL Injection

Las vulnerabilidades en internet pueden ser de muchas formas y colores, una de las más interesantes son las Inyecciones Sql las cuales pueden ser corregidas fácilmente, pero pueden generar muchos problemas si no se detectan a tiempo. Tovar (s.f) define las la inyección de sql como "un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en un aplicación en el nivel de la validación de una entrada para realizar consultas sobre la base de datos". Como se puede ver este tipo de ataque es producto de un problema de diseño del mismo sitio y deja vulnerabilidades en las entradas las cuales los atacantes pueden aprovechar y ejecutar comandos sql y robar información sensible que se encuentra en la base de datos.

Ransomware

Hay momentos donde los ataques son a gran escala y puede generar pérdidas millonarias de un momento a otro, aquí es donde entran los Ataques Ransomware. Estrada (2018) menciona la definición de este concepto es "un programa malicioso que impide el acceso a los ficheros almacenados en el equipo informático y/o al propio sistema informático para solicitar un rescate económico a la víctima si quiere recuperar este acceso".

Este tipo de ataques son complicados de manejar debido a que ocurren de un momento a otro y está en juego uno de los factores más importantes de una empresa, la información de sus clientes, y destruyen claramente los principios de seguridad de acceso a la información y no solo queda ahí, esto se puede ver como si fuera un secuestro de una persona, la guia la tiene el que comete el ataque y los que son víctimas deben ver como hacen para tratar de recuperar lo secuestrado, llegando a pagar

mucho dinero o perdiendo directamente el control de la información, generando pérdida de confianza y grandes sumas de dinero.

DDoS

Hay ciertos ataques que pueden causar un daño extremadamente grande a cualquier empresa que tenga sus servicios en internet, un tipo de ataque que puede colgar el sistema de manera simple y puede que sea por minutos, horas o hasta días, estos ataque son los denominados DoS o DDoS. Haulmer Inc(2018) toma muy en serio este tema, este mismo explica el el objetivo es "consumir los recursos de la máquina o red destino causando la indisponibilidad de sus servicios". Aqui se puede ver el problema que conlleva este tipo de ataque, si imaginamos una empresa en un viernes negro, donde sus ofertas son tan generosas que atraen a todo el publico, un ataque de este tipo puede colgar la pagina y evitar que el proceso normal de compra quede fuera de servicio lo que facilmente puede significar perdidas millonarias de dinero y de credibilidad.

La forma en la que normalmente trabajan los que realizan estos ataques es por medio de "Botnets". Haulmer Inc(2018) define este concepto como "grupo de dispositivos infectados con un *bot* que puede ser gestionado de forma remota". Muchas veces los usuarios del dispositivo nunca se dan cuenta que forman parte del ataque y sus computadores se comportan como zombies.

Adquisición de cuenta

El engaño se produce al obtener datos de un usuario o un cliente y tomar el control de su cuenta, cambiando la dirección postal o el número de teléfono para poder realizar el fraude online.

Robo de identidad

Operación fraudulenta por la que se sustraen datos personales, de contraseñas, nombres de usuario o números de tarjetas de crédito.

Fraude amistoso

Al vendedor le entra una compra y pese a que todo parecía normal, se la devuelven. El cliente estafador ha declarado la compra como fraudulenta en su banco, aunque en realidad fuera él quien ideara la trampa para quedarse con el producto a coste cero.

Reenvio

Un defraudador compra en un comercio online con una tarjeta robada y utiliza una mula para recibir el envío y evitar ser descubierto, remitiéndose a este una vez haya llegado.

Triangulación nociva

El cliente compra un producto a través de una tienda online pirata (el cliente desconoce que es un establecimiento ilegal) y ésta, que no dispone del artículo, se lo encarga a un comercio electrónico legal mediante una tarjeta robada.

Suplantación de Identidad

El estafador engaña al usuario mediante un correo spam, invitándole, por ejemplo, a realizar una operación bancaria a través de una página que aparentemente es de confianza.

Recomendaciones

Si estás pensando en implementar un negocio en línea es de gran importancia contar con las medidas de seguridad adecuadas para proteger tu negocio, ya que los ataques informáticos pueden presentarse cuando menos lo esperas y esto afectará a tus compradores.

Es importante seguir algunos alineamientos y medidas de seguridad que se pueden establecer para proteger tu negocio en línea.

Establece un Firewall perimetral, el cual sirve para proteger y establecer reglas de las entradas de los servicios y salidas en internet.

Asegúrate de contar con un sistema IDS, o sistema de detección de intrusos, lo cual permite el monitoreo de eventos de ataque e informa a un centro de monitoreo para que estés siempre enterado de cualquier situación de riesgo. Es por esto que también es importante implementar configuraciones a nivel estándar de servicios y servidores para asegurar que no quede ninguna configuración por defecto.

También debes contar con un plan de resguardo de información y de contingencia frente a cualquier tipo de desastre; esto es, tener un plan de políticas de resguardo de información diaria o mensualmente, contar con un historial local y fuera de la plataforma.

Crea un protocolo de rescate en caso de desastres; se necesita tener un alineamiento o un seguimiento con instrucciones para recuperar la información perdida en caso de que el sistema falle para que tu empresa no se vea perjudicada en caso de pérdida de información importante.

Caso de estudio

Grupo de hoteles Marriott International

En el año 2018 el grupo de Hoteles Marriott International hizo público el hecho de que sus bases de datos fueron vulneradas por hackers. Este hecho fue alarmante en todo sentido debido a que se informó que desde el 2014 ya habían sido vulneradas y no se habían dado cuenta. Dentro de la información que fue copiada por los atacantes se encontraba información relacionada con nombres, fechas de nacimiento, números de pasaportes, números de tarjetas de cuentas, fechas de vencimiento, entre otros.

Este tipo de problemas son de suma importancia de observarlos, tomando en cuenta la magnitud del nivel empresarial que es el grupo de hoteles Marriot International, si ellos fueron vulnerados a ese punto es porque no se la dio importancia suficiente a la seguridad informática, el hecho de que hasta el 2018 se dieran cuenta de esta filtración de información solo deja entre ver lo mal que están los sistemas que resguardan la integridad y la seguridad de la misma. A raíz de todo se hizo la correspondiente denuncia, pero ya el daño había sido hecho, la imagen de la empresa perdió credibilidad, además muchos clientes demandaron a la empresa, lo cual podría suponer cifras extremadamente altas de dinero que debería pagar.

Por otra parte, se hizo la advertencia de posibles ataques posteriores de phishing a los correos de los usuarios con la premisa de que los correos recibidos eran por parte del grupo de hoteles Marriott International con el fin de llegar a un acuerdo para solucionar la información, pero eran los mismos atacantes aprovechando la oportunidad.

Conclusión

A modo de conclusión podemos decir que la combinación de la autenticación, confidencialidad, integridad y no repudiación como mecanismos de seguridad, descritos anteriormente, permite garantizar con un cierto grado de confiabilidad la seguridad en una transacción electrónica.
Para minimizar los riesgos del comercio electrónico en Internet es necesario conocer algunos conceptos, técnicas y algoritmos que permitan implementar un sistema de seguridad. Es por esto que en este presente tema de investigación explica las técnicas utilizadas por la criptografía, las cuales permiten aumentar el grado de confianza en las aplicaciones de comercio electrónico

El comercio electrónico necesita apoyarse en mecanismos que sean eficaces para así poder garantizar la privacidad y la seguridad de las redes abiertas por tal motivo debe contar con sistemas de seguridad que ayuden a tener un nivel de seguridad seguro en cada sitio o página web

Referencias

INCIBE. (2020, 02 27). *Protege tu empresa*. Consideraciones de seguridad para tu negocio electrónico. Visitado 09 30, 2020, Recuperado https://www.incibe.es/protege-tu-empresa/blog/consideraciones-seguridad-tu-comercio-electronico

CECARM. (2010, 05 02). *Guia seguridad en el comercio electrónico*. Seguridad en el comercio electrónico. Visitado 09 30, 2020, Recuperado https://www.cecarm.com/Guia_Seguridad_en_el_comercio_electronico_-_CECARM.pdf-6559#:~:text=Para%20asegurar%20las%20transacciones%20en,transmiten%20a%20trav%C3%A9s%20de%20Internet.

sf. (n.d.). *Seguridad en el Comercio Electrónico*. Comercio Electrónico. Visitado 10 08, 2020, Recuperado https://sites.google.com/site/webcelectronico/-en-que-consiste-el-comercio-electronico/seguridad-en-el-comercio-electronico

Santiago, H. J. G. (2004). *Seguridad en el Comercio Electrónico* (Primera ed., Vol. 81). https://www.javeriana.edu.co/biblos/tesis/derecho/dere6/DEFINITIVA/TESIS24.pdf

Edgar Higuerey. (2019, 07 01). *¿Qué es el comercio electrónico y cuales son sus ventajas?* Comercio electrónico: conoce todo sobre este modelo de negocios y cuáles son sus ventajas. Visitado 10 08, 2020, Recuperado https://rockcontent.com/es/blog/comercio-electronico/

Watson, W. T. (2020, 07 31). *Riesgos Ecommerce*. Ecommerce: Riesgos a los que se enfrentan los e-vendedores. Visitado 10 08, 2020, Recuperado https://willistowerswatsonupdate.es/ciberseguridad/e-commerce-riesgos-enfrentan-e-vendedores/

Valencia, O. T. (n.d.). *Ataques*. Inyección de SQL, tipos de ataque y prevencion en ASP.NET C#. Visitado 10 26, 2020, Recuperado http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2948/Trabajo%20de%20grado.pdf?sequence=1

Cola, C. E. (2018, 12 01). *Estudio sobre el malware Ransomware*. Estudio sobre el malware Ransomware. Visitado 10 27, 2020, Recuperado http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89025/6/cestradacolTFM0119memoria.pdf

BBC News Mundo. (2018, 11 28). *Marriott: un ataque informático deja expuestos los datos de 500 millones de clientes del grupo hotelero*. Ataque informático. Visitado 10 25, 2020, Recuperado https://www.bbc.com/mundo/noticias-46404767

Haulmer Inc. (n.d.). *Introducción a los ataques DDoS y métodos Anti-DDoS*. DDoS y Anti-DDoS. Visitado 10 26, 2020, Recuperado https://www.haulmer.com/docs/introduccion-a-los-ataques-ddos-y-metodos-anti-ddos/

El Financiero. (2015, 05 22). *Firma Digital*. 11 trámites que puede hacer un emprendedor con la firma digital. Visitado 10 26, 2020, Recuperado https://www.elfinancierocr.com/pymes/11-tramites-que-puede-hacer-un-emprendedor-con-la-firma-digital/76Z4TNIS6FEBFJATIES4W45GZ4/story/#:~:text=En%20el%20Banco%20Nacional%20de,PIN%20o%20desbloqueo%20cuesta%20%245

Firma Digital. (n.d.). ¿Qué es la Firma Digital? Visitado 10 26, 2020, Recuperado https://www.mifirmadigital.go.cr/

R, C. L. (2018, 04 09). *Seguridad en eCommerce*. Seguridad en eCommerce: Protege a tus Clientes y a tu Empresa. Visitado 10 26, 2020, Recuperado https://blog.niumedia.mx/seguridad-en-ecommerce