Universidad Nacional Autónoma de México
Facultad de Contaduría y Administración
Sistema Universidad Abierta y Educación a Distancia

Desarrollo de Sitios web con Transacciones en línea

Actividad 1, Unidad 6: Creando un carrito de compras

Elaborado por:
Metztli Huertero Granada
No. de cuenta: 420145763

Licenciatura en Informática
Semestre 2024-2

Actividad 1, Unidad 6: Creando un carrito de compras

Introducción

Una vez que una empresa cuenta con una interfaz amigable y una arquitectura de sitio web que permita a sus usuarios navegar cómodamente y los motive a efectuar una compra, es necesario implementar un sistema de pago y la protección informática que asegure el manejo ético, transparente y correcto de datos personales sensibles, como lo son los datos bancarios, nombre completo o el domicilio del cliente. En esta actividad, se desarrollan de manera teórica los principios de los mecanismos, medios y sistemas de pago, así como los fundamentos de seguridad informática aplicables a los sitios web con transacciones en línea.

Desarrollo de la actividad

Arquitectura de un carrito de compras

El carrito de compras es el elemento base para el funcionamiento de los comercios electrónicos, pues es la herramienta que permite al usuario crear un listado de compra, visualizar y aceptar el pedido de bienes o servicios, procesar la compra y concretar el pago. En otras palabras, posibilita la compra en Internet, ofreciendo una interfaz amigable, intuitiva y que facilita el proceso de efectuar una transacción en línea.

Para la creación de un carrito de compras debemos de considerar los elementos técnicos que permitirán su correcto funcionamiento, los cuales conforman la arquitectura del mismo. Éstos son: el diseño estético e interactivo de la página (*frontend*), la lógica de negocio y procedimientos técnicos-programáticos (*backend*), la estructura y diseño del espacio donde se almacenarán las entradas de datos a la página (base de datos), entre otras herramientas y adiciones que permitan efectuar

una transacción dentro de sitio, como las pasarelas de pago. El siguiente gráfico resume las aplicaciones de cada componente:

Integrando todos estos elementos, es posible crear un carrito de compras que permita incorporar y eliminar productos, hacer la comprobación de los ítems seleccionados antes de efectuar la compra, hacer el pago correspondiente, e incluso establecer conexión con el departamento o el sistema de gestión de inventarios y envíos.

En los siguientes apartados se hablará de manera detallada acerca de los mecanismos, medios y sistemas de pago, así como conceptos fundamentales para asegurar el circulamiento seguro de información bancaria dentro de nuestro sitio de e-commerce.

Herramientas para construir un carrito de compras

Cada nivel en la arquitectura del carrito de compras ocupa diferentes tecnologías, herramientas y marcos de trabajo en los que se basa para cumplir con su función. El siguiente cuadro menciona las herramientas utilizadas en cada categoría, así como su función general para el funcionamiento de un carrito de compras:

Tabla 1.1. Tecnologías y herramientas empleadas para el desarrollo de un carrito de compras virtual	
Tecnología	**Descripción**
***Frontend** (parte con la que tiene contacto el cliente)*	
HTML	Lenguaje de etiquetas de hipertexto; permite seleccionar y estructurar el contenido de la página. Conecta a todas las tecnologías de frontend utilizadas.
CSS	Hoja de estilo en cascada; da estilo, estética y funciones visuales al contenido HTML.
JavaScript	Lenguaje de programación que da dinamismo al sitio web, implementando mecanismos de animación, transiciones, validación de formularios, acción de botones, y respuesta a las interacciones del usuario con el sitio web.
React	Una biblioteca de JavaScript que agiliza la navegación entre sitios web, la gestión del carrito de compra y los ítems en él.
Angular	Framework utilizado para la creación tanto de aplicaciones web como móviles; se suele implementar para dar mayor dinamismo a la página, a los menús, y la reutilización de código.

***Backend** (procesamiento de datos; lado del servidor)*	
Java, Python, Node.js	Lenguajes de programación que permiten manipular las entradas del sitio web, dadas por los usuarios, y procesarlas según la manera en la que el usuario interactuó con la página; programa del lado del servidor.
PHP	Lenguaje de programación que ejecuta funciones según las peticiones/interacción del usuario, pero que no serán percibidas por él. Permitirá tener control de lo que se ingresa en el carrito, eliminar un producto, mostrar el carrito, entre otros métodos.
Spring Framework	Un framework aplicado a Java para la agilización del proceso de codificación en el lenguaje de programación; ofrece bloques de código con procesos repetitivos; también incluye herramientas de gestión de seguridad.
Django	Framework escrito con lenguaje Python que busca que la programación del sitio web sea segura, versátil y rápida. Ofrece módulos de código para la administración de cuentas de usuario, autenticación,
Bases de datos	
SGBD	Un sistema gestor de bases de datos, permitirá crear una base de datos para registras, modificar, almacenar y eliminar información relevante para el funcionamiento del carrito de compras.

Sistema de pago	
Pasarelas de pago	Un servicio que conecta a la tienda virtual con una plataforma que facilita y autoriza el pago de los servicios o bienes que fueron agregados al carrito dentro del sitio web del e-commerce.
Seguridad informática	
Firewalls	Un software integrado para proteger a las transacciones en línea: que no sean interceptadas, modificadas, o canceladas por conexiones externas a los enlaces predefinidos en el sitio web y sus servidores; desvía todo tráfico de red malicioso.
SSL/TLS, HTTPS	Protocolos de seguridad que se encargan de cifrar la información que se comparte en una comunicación o enlace cliente-servidor; se cifra todo el contenido de la página al implementar HTTPS, además de la información personal sensible de los clientes, específicamente al implementar SSL/TLS.
JSON Web Tokens	Un estandar que define los métodos para el intercambio de información seguro entre una comunicación cliente-servidor; permite autenticar al cliente cada que necesita ejecutar una acción que necesita verificar su identidad, enviando en cada una de estas acciones un token que contiene las credenciales que validan la identidad del usuario.

Fundamentos de mecanismos de pago

Ya sea que adoptemos el rol de cliente o de vendedor, es necesario estar familiarizado con los mecanismos, sistemas y medios de pago que existen en el mundo digital ya que, conforme pasa el tiempo, nos encontramos con mecanismos de pago cada vez más variados, pero que buscan simplificar aún más el proceso de pago en el comercio digital.

El tema de fundamentos de mecanismos de pago hace referencia a **todos los elementos involucrados en la transferencia de dinero** como parte de una transacción comercial entre dos partes, ya sea en el entorno físico o digital. Dado que el comercio digital busca adecuar y adaptar el comercio tradicional al entorno virtual, los mecanismos de pago como los cheques, las transferencias y tarjetas bancarias, los pagarés, recibos o domiciliaciones de pago deben también transformarse para seguir manteniendo su vigencia, interés y relevancia en el mercado.

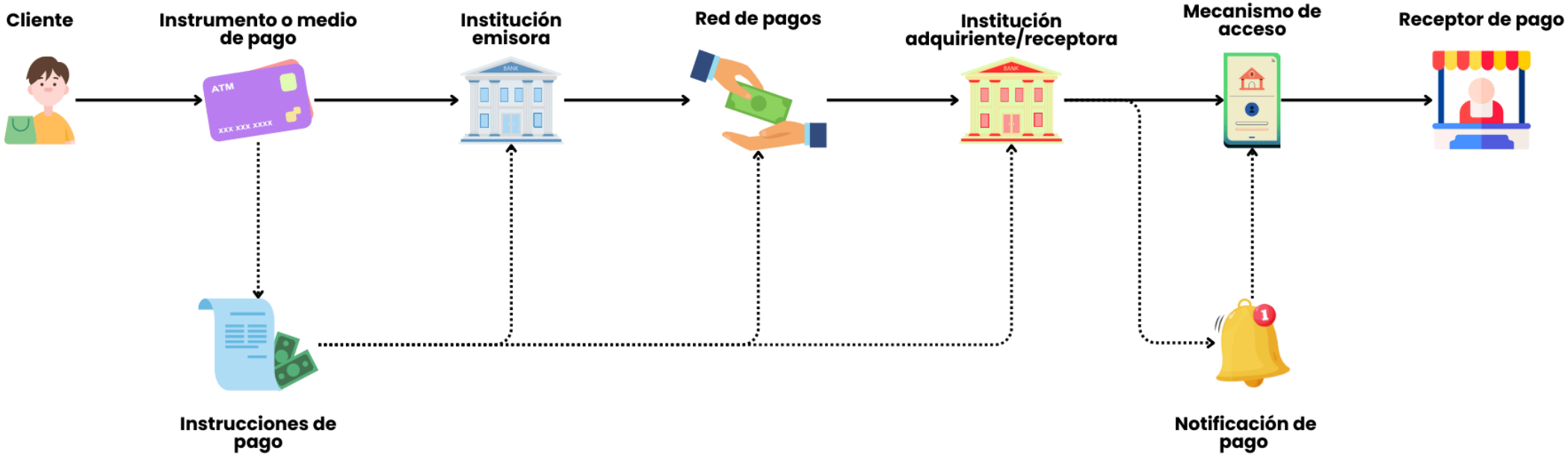
Sistema de pago electrónicos

Los sistemas de pago electrónicos están compuestos por todos aquellos **elementos que posibilitan las transacciones de dinero sin la necesidad de que éste se tenga de manera física**, y toman relevancia cuando se habla de comercio electrónico, pues benefician al e-commerce al poder intercambiar un bien o servicio y su valor monetario en dinero sin ser necesaria la presencia física de los vendedores y los clientes para llevar a cabo tal transacción. Un punto clave para el éxito del comercio electrónico es el uso de sistemas de pago seguros y eficientes (Pegueroles, 2002).

Existe una variedad de sistemas y medios electrónicos de pago, sin embargo, todos ellos involucran los siguientes procesos:

Sistemas de Pago

Elaborado por: Metztli Huertero Granada



Tipos de sistemas de pago

En la actualidad, existe una gran variedad de plataformas y tecnologías diseñadas para facilitar y procesar las transacciones financieras que se generan en el sitio web de un comercio digital. Entre las mas relevantes, se encuentran:

- **SPEI,** los Sistemas de Pagos Electrónicos Interbancarios es desarrollado por el Banco de México en conjunto con otras instituciones bancarias del país. Su objetivo principal es posibilitar en envío bidireccional de dinero entre cuentas bancarias, vía electrónica, aún siendo las cuentas de diferentes bancos. Se rige de reglas que estableció BANXICO, que delimita, por ejemplo, el horario en el que se puede efectuar un envío vía banca por Internet, o el tiempo límite de recepción de pagos.
- **Plataformas de pago,** son los sujetos intermediarios entre el cliente, las instituciones financieras, y el vendedor. Dicho de otra manera, se encarga de ingresar al sistema de pago electrónico de manera segura, aprobando la transacción y verificando que la información proporcionada por el cliente esté completa y correcta (esta es la función de una pasarela de pago, misma que está integrada en una plataforma). Así mismo, las plataformas de pago suelen contar con herramientas de gestión de inventario, pedidos, y de análisis de datos por ventas. La plataforma de pago más utilizada en la actualidad es Shopify.
- **Carteras electrónicas,** también llamada billetera electrónica o e-wallet, es la virtualización de una cartera tal y como la conocemos: tiene la función de almacenar los datos de las tarjetas de crédito y débito en una aplicación e-wallet. Ésta podrá ser utilizada tanto para compras en línea como para los pagos sin contacto, con el teléfono móvil.

Medios electrónicos de pago

Los métodos de pago electrónicos son las herramientas financieras que permiten ejecutar una transacción en línea, a través de un dispositivo conectado a Internet. A lo largo de toda la historia del e-commerce, el medio principal para concretar los pagos en línea han sido las tarjetas de crédito y débito, y conforme este modelo de negocio ha ido evolucionando e incorporado nuevas tecnologías ,los métodos de

pago también han sufrido modificaciones que han vuelto a las transacciones en línea procesos seguros, transparentes y ágiles.

En la siguiente tabla, se incluyen las características fundamentales de cada medio de pago, y al menos, dos plataformas o tecnologías involucradas en él:

Tabla 1.2. Medios electrónicos de pago		
Método de pago	**Descripción**	**Ejemplo**
Tarjetas crédito/débito	Cuando se paga directamente con una tarjeta de crédito o débito, no existe un redireccionamiento a una plataforma de pago auxiliar, sino que la transacción se efectúa en el mismo sitio. Existen métodos de compra seguros que implican la creación de tarjetas virtuales con datos bancarios dinámicos, que protegen la confidencialidad de los datos financieros del cliente.	• Visa • MasterCard • American Express
Transferencias electrónicas	Que se llevan a cabo mediante una pasarela de pago, a la cual se tiene acceso mediante un redireccionamiento a la página donde se llevará a cabo la transacción, y los datos financieros del cliente se	• PayPal • Stripe

	protegen mediante un proceso de encriptamiento.	
Pago en efectivo	Existen comercios electrónicos que generan claves de pago, con el fin de generar una transacción en línea con una institución autorizada, y que ésta reciba el dinero en efectivo.	Pago en establecimientos autorizados, como Oxxo, Walmart, 7Eleven.
Compra ahora, paga después	Un método de pago el cual emite un préstamo que cubre el total de la compra en el e-commerce, para posteriormente ofrecer a cliente un esquema de pagos quincenal.	● KueskiPay ● Klarna
Criptomonedas	Llamadas también monedas digitales, generadas por software especializado y algoritmos complejos. Las criptomonedas pueden ser transferidas entre “iguales” sin la necesidad de instituciones intermediarias como los bancos.	● Bitcoin ● Ethereum
Tarjetas de regalo o prepago	Las cuales se pueden adquirir en tiendas de conveniencia, y cargadas con el saldo indicado	Tarjetas de regalo de Amazon, Paypal.

	al momento de pagar por ella. Pueden ser utilizadas en diferentes plataformas, aplicaciones; incluso algunas de ellas funcionan como una tarjeta de débito de un sólo uso.	

Fundamentos de seguridad informática

Estamos conscientes que, en la actualidad, los recursos más valiosos son los activos informáticos, es decir, todos aquellos dispositivos que permiten ingresar, procesar, analizar, almacenar, visualizar y disponer de información en formato digital, y la propia información. Por ello, es fundamental conocer y aplicar medidas que permitan proteger estos recursos de las malas prácticas, de comportamientos no autorizados y la manipulación inapropiada de la informática y sus herramientas.

La seguridad informática toma como principal preocupación la protección de la red informática en sus tres niveles conceptuales (hardware, software, información) ante cualquier vulnerabilidad de la misma. Vivimos en una época en la cual la ciberseguridad, que abraza a la seguridad informática junto con otros enfoques, debe de tener una presencia indiscutible en comercios, empresas, instituciones, incluso en los dispositivos, sistemas y servicios particulares, pues toda la información que circula en la red, tanto pública como privada, es vulnerable a cualquier tipo de filtración, ataque o robo.

El campo de acción de las medidas de seguridad informática suele ser amplio, pues a menudo una variedad de tecnologías se interrelacionan para formar una infraestructura de seguridad compleja y segura. Disciplinas como seguridad de red, de aplicaciones, de la nube y de dispositivos finales son algunas de las involucradas, además de seguridad física de la empresa, protegiendo la autenticación y autenticidad de los datos, personas y dispositivos que operan en la organización.

Las principales amenazas a la seguridad informática se resumen a continuación:

- **Ataques de Ingeniería social**: Los cuales ocurren bajo un ambiente de confianza falso, impuesto por el atacante. El fin de estos ataques es obtener acceso a la información privada y confidencial de la empresa mediante la manipulación de las personas autorizadas para tener acceso a los recursos informáticos, Google enlista cuatro ataques de ingeniería social comunes:
    - ***Suplantación de identidad***, un ataque que suele ser concurrente, en donde los atacantes tienen acceso a las credenciales de una persona de alto rango en una empresa, o bien, tienen las herramientas para hacerse pasar por tal persona, para engañar a otros empleados y conseguir información confidencial.
    - ***Cebo USB***, ataque que se lleva a cabo dentro de una empresa, en donde se deja una USB perdida o con aparente información confiable e importante, esperando que quien la encuentre, la conecte a un equipo organizacional para infectarlo con software malicioso.
    - ***Ingeniería social física,*** que ocurre haciéndose pasar por un empleado importante en la empresa para tener acceso a áreas restringidas, siempre con el fin de obtener información confidencial o causar un daño en la infraestructura informática.
    - ***Phishing***, el ataque que puede englobar a los tres anteriores, consiste en el uso de diferentes medios de comunicación, como correos, llamadas telefónicas, SMS, para engañar y convencer al destinatario a compartir credenciales de autenticación e identificación, enviar dinero, o descarguen e instalen software malicioso. Se suelen clasificar según el medio utilizado y por el sujeto objetivo.
- **Ataques de puerta trasera**: Un tipo de ataque a considerar, más aún cuando somos desarrolladores de un sistema o plataforma de uso empresarial. Se les llama puerta trasera son los accesos débiles al sistema, pensados para el uso de los administradores del sistema, para su fácil ingreso a la plataforma y realizar las modificaciones que éste requiera. Sin embargo, esta también es una vulnerabilidad que pone en riesgo a la información de la empresa, puesto que los ciber atacantes pueden aprovechar esta entrada fácil y ejecutar cualquier tipo de acción maliciosa.

- ***Software malicioso***, nombrado también como malware, son todos aquellos programas que alteran el funcionamiento regular del sistema, lo estresa o bloquea, con el fin de acceder a la información de valor. Entre los ataque de malware más comunes son el ransomware, el spyware y los gusanos.
- ***DoS***, los ataques de denegación de servicio, o nombrados coloquialmente como *doseo*, se encargan de estresar a un sistema mediante el envío de cantidades inmanejables de tráfico, para después implantar en el software malicioso.
- ***Ataques de día cero,*** en donde los atacantes identifican una brecha de seguridad que los dueños o desarrolladores del sistema desconocen y se aprovechan de ella para efectuar un ataque. Son amenazas que no son descubiertas a tiempo, y sólo se hacen visibles cuando el ataque ya fue ejecutado, por lo que los desarrolladores no tuvieron el tiempo para corregirlo.

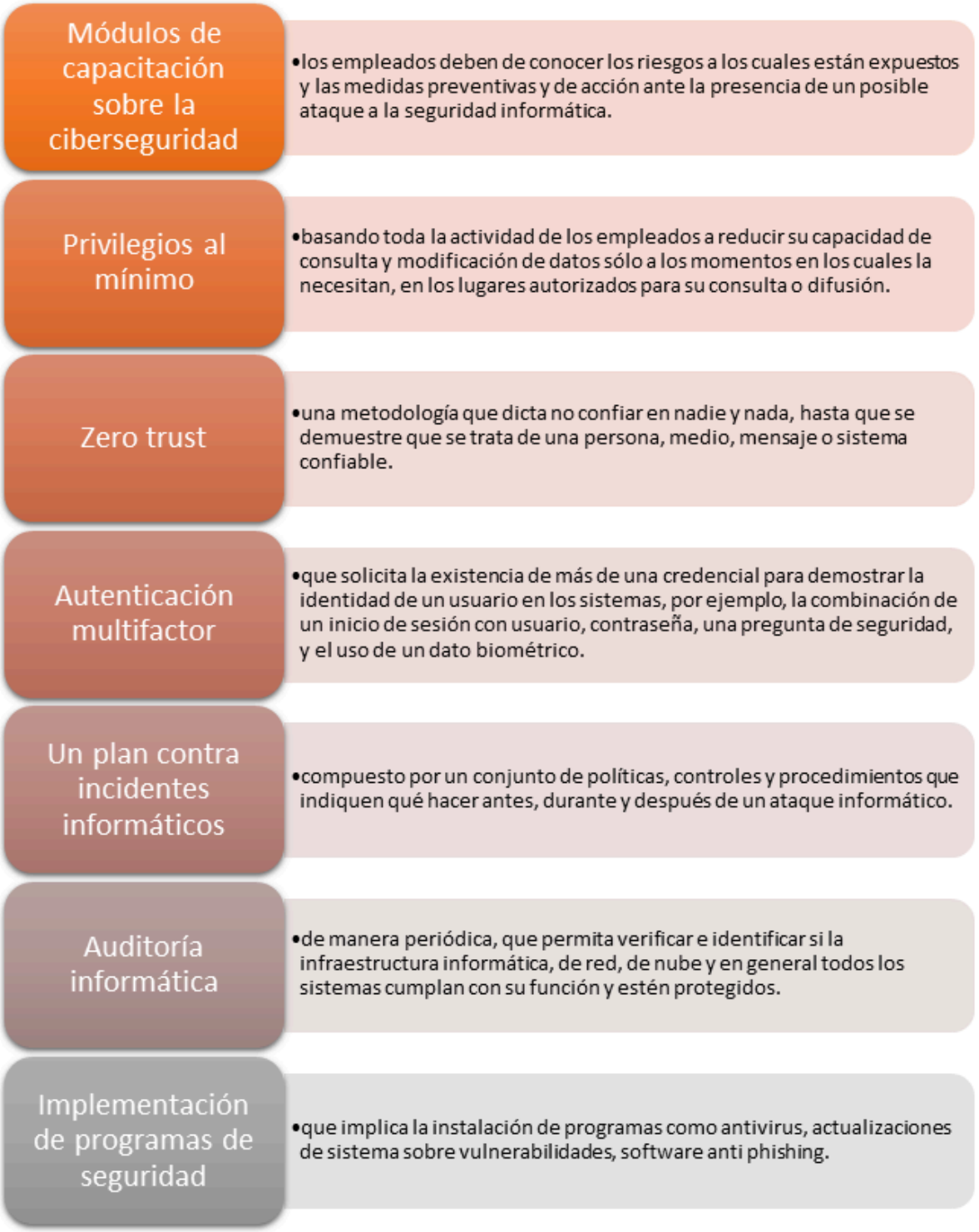
Mecanismos de seguridad

Cómo informáticos, debemos de ser conscientes de las repercusiones que la ausencia de medidas de seguridad informática en la operación de un negocio, una empresa, una organización, provoca. Es importante mencionar que la falta de mecanismos de seguridad pueden impactar fuertemente en la economía y financiamiento de la institución; en su reputación y credibilidad social; en su presencia mercantil; en la continuidad de su negocio. IBM menciona en una de sus cápsulas IBM Think que Los ataques cibernéticos y los incidentes de seguridad pueden cobrarse un precio enorme medido en pérdidas de negocio, reputación dañada, multas reglamentarias y, en algunos casos, extorsión y robo de activos[1].

Para evitar la pérdida de recursos económicos y activos importantes, es necesario considerar una variedad de buenas prácticas y mecanismos de seguridad que permitan proteger en todas sus dimensiones a la infraestructura informática. A nivel

[1] IBM (s.f). **"¿Qué es la seguridad informática?. Cuál es la importancia de la seguridad informática"**. IBM Think.

empresa, negocio u organización, éstas son algunas de las medidas que se pueden implementar:



Seguridad digital

Además del enfoque de seguridad informática, también consideramos a la seguridad digital como un pilar en la ciberseguridad aplicada a las operaciones comerciales en línea. La seguridad digital tiene por objetivo la implementación de medidas y mecanismos de seguridad a la actividad que se genera en el entorno web: la privacidad en línea, la protección de la identidad, la seguridad en las transacciones virtuales son algunas de sus implicaciones.

Como tal, la seguridad digital se encarga de la protección de la información personal sensible de un usuario en línea, tales como:

- **Datos personales**, todo aquél dato que brinde información sobre la identidad y ubicación de una persona, como lo son el nombre completo, domicilio, número de teléfono, identificador nacional (CURP, clave de elector), correo electrónico, dirección IP.
- **Datos financieros**, relacionados con toda la información confidencial bancaria de una persona, los cuales suelen ser el blanco de los ataques cibernéticos: números de cuenta, datos de tarjetas de cŕedito/débito, incluso el saldo actual en la cuenta de banco.
- **Datos médicos**, los cuales son buscados por los ciberdelincuentes para reclamar seguros médicos, medicinas, o algún otro tipo de práctica relacionada con la suplantación o robo de identidad: número de seguridad social, historial médico, contratación de seguros médicos.

Tanto la Información de Identificación Personal (PII, por sus siglas en inglés) como la Información de Identificación Personal (SPII, por sus siglas en inglés) deben de ser resguardadas, controladas y vigiladas por las instituciones que las manejan, las cuales son, normalmente, del giro bancario, gubernamental, comercial, o plataformas de interacción social (redes sociales). En el siguiente apartado se habla sobre medidas de protección para la creación de plataformas regidas por los principios de Confidencialidad, Integridad y Disponibilidad de la información, tres elementos que conforman una guía de implementación de seguridad en el medio digital, llamada en ciberseguridad como la **Triada CID:**

- **Confidencialidad**, en donde los usuarios de la información necesitan de autorización explícita para acceder a los datos, los cuales están protegidos de las personas que no tengan el permiso de su consulta.
- **Integridad**, los datos estando en reposo o en circulación deben de mantenerse en su estado actual, esto quiere decir que no pueden ser alterados, eliminados o intervenidos de ninguna manera. Dicho de otra forma, es demostrar la autenticidad y confiabilidad de la información.
- **Disponibilidad**, la información sólo será accesible para las personas o áreas empresariales con permiso para visualizarla, consultarla y modificarla, de igual forma que ésta deberá de estar siempre disponible para ellos cuando requieran de su uso.

Mecanismos para aplicaciones seguras de comercio electrónico

Como se mencionaba en secciones anteriores, es fundamental que los comercios electrónicos, así como otras instituciones y organizaciones que manejen el uso de datos personales sensibles, cumplan con principios, prácticas y normas que aseguran el circulamiento seguro de esta información en internet, así como dotar a los clientes de tranquilidad y confianza en la marca, demostrando que la empresa es coherente con su imagen y credibilidad.

El siguiente listado contiene algunas prácticas básicas, tanto preventivas como correctivas, que deben de ser implementadas en las plataformas y sitios web de e-commerce para asegurar que éste sea un ecosistema seguro y protegido contra amenazas externas, acciones delictivas y malas prácticas:

- Acciones básicas:
    - ***Actualizaciones de software y tecnologías***, pues es necesario que siempre se cuente con la infraestructura tecnológica en su última versión, pues las actualizaciones siempre incorporan correcciones ante errores y vulnerabilidades identificadas.
    - ***Creación de backups,*** aún más cuando se trate del codigo fuente del sitio web y sus actualizaciones, las bases de datos vinculadas a los pedidos y datos de operación de la empresa.

- ***Implementación de métodos de autenticación multifactor antes de efectuar una transacción***, lo cual se hace con el objetivo de proteger el dinero y los datos bancarios del cliente antes de hacer el cobro por los productos seleccionados en el carrito. Es fundamental que exista un método para verificar la identidad del cliente que está efectuando la transacción.
- ***Implementación de pruebas de ciberseguridad,*** en donde se evalúen e identifiquen los puntos débiles del sitio web o plataforma que sostiene la operación virtual del e-commerce, buscando cuáles pueden ser vulnerabilidades que representen un riesgo para la operación del sitio, y del negocio en general.
- ***Implementación de protocolos de red de seguridad,*** que aseguren que la comunicación entre el cliente y el comercio electrónico sea segura. Por ejemplo, asegurarse de que el sitio web utilice HTTPS para una navegación segura; incorporar los certificados SSL/TLS para cifrar los datos en tránsito.

- Otras medidas:
  - ***Solicitar al cliente su CVV,*** esto reduce en una cantidad considerable el número de fraudes o compras no autorizadas en sitios web, ya que éstas suelen ocurrir incluso si se cuenta únicamente con el número de tarjeta y fecha de vencimiento.
  - ***Recomendación de uso de tarjetas virtuales/dinámicas,*** que integra en el proceso de compra un nivel más de seguridad: los atacantes, aunque cuenten con los datos bancarios del cliente, éste puede generar desde su banca móvil una tarjeta virtual con la cual efectuar sus compras de manera segura. Algunas se autodestruyen, otras pueden activarse y desactivarse cuando sea necesario.
  - ***Ofrecer al cliente alternativas de pago***, algo que los clientes buscan con frecuencia es que los sitios de e-commerce cuenten con una variedad, no exagerada, de medios de pago, lo cual dota al negocio con un nuevo grado de confiabilidad.

- ***La información del sitio web debe de ser clara, consisa, confiable***, en especial, la que describe a los productos en venta, de modo que el cliente sepa qué es lo que está comprando y bajo qué condiciones será entregado, cuál es el contenido real del producto, cómo se llevan a cabo las transacciones en línea, entre otros detalles.
- ***Informar a los clientes sobre los peligros en Internet***, suele ser muy bien recibida la información que prepara a los usuarios de la gran red ante situaciones desafortunadas, como el robo de información personal sensible, en especial, cuando está relacionada con la relación que adquieres con la empresa. Esta también es una medida innovadora para dar un tipo de contenido de calidad y retribución a los clientes, al realizar una compra en el sitio web.

Conclusión

En esta actividad pude identificar muchas áreas de oportunidad para mi trabajo final; llevo, para el momento de elaboración de este documento, gran parte del frontend de mi sitio web, sin embargo, quisiera crear un proyecto lo más correcto posible, siguiendo todos los principios de ciberseguridad que son necesarios para llevar a cabo una transacción en línea de forma segura. Es probable que mi proyecto final tenga incorporada alguna página con información valiosa sobre la ciberseguridad y la seguridad digital, así como que integre una pasarela de pago, pero en el futuro, quisiera seguir aportando a mi trabajo para llegar al punto de crear proyectos parecidos, con funcionalidad y oportunidad de implementación para un comercio real.

Fuentes de Consulta

Aroca, F (2010). ***“DISEÑO E IMPLEMENTACIÓN DE UNA TIENDA VIRTUAL”.*** Universitat Politécnica de Valencia. https://m.riunet.upv.es/bitstream/handle/10251/9110/dise%C3%B1oeimplementaciondeunatiendavirualFcoAroca.pdf?sequence=1&isAllowed=y

Bank of America (s.f). ***"¿Qué es una Billetera Digital?"***. Mejores Hábitos Financieros. https://bettermoneyhabits.bankofamerica.com/es/personal-banking/what-is-a-digital-wallet

BBVA (2024). ***"¿Qué es SPEI y cómo usarlo?"***. BBVA, Educación Financiera. [Blog]. https://www.bbva.mx/educacion-financiera/creditos/que-es-spei.html

CECARM (febrero, 2010). ***"Seguridad en el comercio electrónico"***. https://www.cecarm.com/Guia_Seguridad_en_el_comercio_electronico__CECARM.pdf-6559

Clip (30 de agosto, 2023). ***"Cuáles son las opciones para recibir pagos en línea"***. [Blog]. https://blog.clip.mx/articulo/cuales-son-las-opciones-para-recibir-pagos-en-linea

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (1 de marzo, 2022). ***"Pagos electrónicos y digitales"***. Revista Proteja su Dinero pp 42-44. https://revista.condusef.gob.mx/wp-content/uploads/2022/03/pagos_264.pdf

Conekta (2 de febrero, 2023). ***"Seguridad del comercio electrónico: Todo lo que debes saber"***. Equipo Editorial Conekta [blog]. https://www.conekta.com/blog/seguridad-comercio-electronico

Del Hoyo, J (13 de enero, 2024). ***"Tienda Online:WebCine".*** Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/27001/5/jdelhoTFC0114memoria.pdf

Dirección General de la Incorporación y Revalidación de Estudios (s.f). **"Seguridad Digital"**. UNAM. Consultado el 15 de mayo del 2024. https://www.dgire.unam.mx/webdgire/contenido_wp/documentos/seguridadescolar/tecnologia-informacion-definicion.html

Hewlett Packard Enterprise (2024). **"¿Qué es la seguridad Informática?"**. Hewlett Packard Enterprise Development . [blog].https://www.hpe.com/mx/es/what-is/it-security.html#:~:text=La%20seguridad%20inform%C3%A1tica%20se%20encarga,gracias%20a%20la%20seguridad%20inform%C3%A1tica

IBM (s.f). **"¿Qué es la seguridad informática?"**. IBM Think. Consultado el 15 de mayo del 2024. https://www.ibm.com/mx-es/topics/it-security

Kueski (2024). ***"¿Qué es Kueski Pay?"***. Kueski Pay. https://preguntas.frecuentes.kueski.com/hc/es/articles/14765228542363--Qu%C3%A9-es-Kueski-Pay

Mailchip (2023). ***"¿Cuáles son los beneficios de los carros de compra en línea?".*** Intuit Mailchip [blog]. https://mailchimp.com/es/resources/what-is-online-shopping-cart/

MIPYMESMX (2020). ***"Comercio digital. Sistema de pago".*** Secretaría de Economía. https://mipymes.economia.gob.mx/wp-content/uploads/2020/12/4.4-HETD.pdf

Nodenet (13 de marzo, 2021). ***"¿Qué es una plataforma de pago y cómo funciona en tu Ecommerce?"***. [Blog]. https://nodenet.es/blog/que-es-una-plataforma-de-pago-y-como-funciona-en-tu-ecommerce

Obando, R (15 de septiembre, 2023). ***"Carrito de compras online: qué es y cómo crearlo paso a paso".*** HubSpot [blog]. https://blog.hubspot.es/sales/carrito-de-compras#que-es

Santos, J (24 de septiembre, 2023). ***"6 consejos para mejorar la seguridad del comercio electrónico"***. Delta Proyect [blog]. https://www.deltaprotect.com/blog/seguridad-del-comercio-electronico

Stripe (27 de marzo, 2023). ***"Métodos de pago de e-commerce: qué son y cómo elegir los adecuados"***. [Blog]. https://stripe.com/mx/resources/more/ecommerce-payment-methods#tipos-de-metodos-de-pago-de-e-commerce

Stripe (3 de octubre, 2023). ***"Sistemas de pago por Internet: diferencias y funciones"***. [Blog]. https://stripe.com/mx/resources/more/online-payment-systems

Vélez, C (2024). **"Seguridad Informática"**. Instituto de Ingeniería, FI UNAM. https://www.iingen.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/seguridadinformatica.aspx

ZRUpay (2024). ***"¿Qué es un e-wallet o una billetera electrónica?"***. [Blog]. https://www.zrupay.com/blog/que-es-ewallet