UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DEPARTAMENTO DE COMPUTACIÓN Y SIMULACIÓN DE SISTEMAS

Nombre del curso:

Desarrollo IX

Tema:

Comercio Electrónico

Integrantes:

Madelaine Arosemena 8-1004-668

Javier Hernández 8-1001-178

Joel Castillo

Profesor:

Erick Agrazal

Fecha de entrega:

19/04/2025

Introducción

En el entorno del comercio electrónico, la infraestructura tecnológica desempeña un papel crucial para el éxito de cualquier plataforma digital. Este documento aborda los aspectos esenciales que deben considerarse para garantizar un funcionamiento óptimo: la elección y gestión de un proveedor de servicios de internet (ISP), el diseño y mantenimiento de una base de datos eficiente, los distintos métodos de pago disponibles, y las prácticas de seguridad necesarias para proteger la información sensible y garantizar la confianza del cliente.

Índice

Como elegir y trabajar con un ISP

La elección del proveedor de servicios de internet (ISP) es una decisión estratégica para cualquier empresa que opere un sitio de comercio electrónico. La calidad y confiabilidad del servicio contratado influye directamente en el rendimiento de la plataforma, la satisfacción del cliente y la continuidad del negocio. A continuación, se detallan los factores clave que deben ser considerados al seleccionar y colaborar con un ISP:

- **Velocidad de conexión:** En el comercio electrónico, la rapidez en la carga del sitio y en la gestión de transacciones es fundamental. Una conexión lenta puede afectar negativamente la experiencia del usuario y provocar la pérdida de ventas. Por tanto, es importante que el ISP ofrezca planes con velocidades de carga y descarga suficientes para soportar procesos como la carga de productos, el manejo de inventario y el procesamiento simultáneo de pagos.

- **Estabilidad y fiabilidad:** Además de la velocidad, la estabilidad del servicio es un aspecto crítico. Un ISP confiable debe garantizar un alto porcentaje de disponibilidad (uptime), minimizando interrupciones que puedan afectar el funcionamiento del sitio web. Asimismo, debe contar con tiempos de recuperación ágiles ante fallos, lo que resulta crucial para evitar pérdidas operativas.

- **Escalabilidad del servicio:** A medida que el sitio crece en volumen de usuarios y datos, también aumentan las necesidades de conectividad. Por ello, resulta ventajoso contar con un proveedor que permita escalar los recursos fácilmente, sin necesidad de cambiar de infraestructura o enfrentar interrupciones.

- **Seguridad de la red:** La protección de datos sensibles, tanto de la empresa como de los clientes, es una prioridad en el comercio electrónico. Algunos ISP ofrecen servicios adicionales como cortafuegos (firewalls), filtros contra software malicioso y medidas contra ataques de denegación de servicio (DDoS), lo cual agrega una capa extra de seguridad a la operación digital.

- **Soporte técnico:** Es esencial contar con soporte técnico eficiente y disponible en todo momento. Los proveedores deben ofrecer atención 24/7 y múltiples canales de contacto, como chat en línea, teléfono o correo electrónico, lo cual permite atender con rapidez cualquier problema que afecte la conectividad o el rendimiento del sitio.

- **Cobertura y factibilidad del servicio:** En algunas ubicaciones geográficas, especialmente en zonas rurales o de difícil acceso, los servicios tradicionales como la fibra óptica pueden no estar disponibles. En estos casos, es necesario evaluar ISPs que ofrezcan soluciones alternativas adaptadas a la ubicación de la empresa, garantizando la conectividad sin depender de largos tiempos de instalación o infraestructura costosa.

- **Consideraciones económicas:** El costo del servicio debe analizarse cuidadosamente. Más allá del precio mensual, deben tenerse en cuenta posibles tarifas por instalación, alquiler de equipos, penalizaciones por cambios en el contrato o límites en el uso de datos. La elección debe equilibrar calidad del servicio con sostenibilidad financiera.

Consideraciones de la Base de Datos

Una base de datos eficiente es fundamental para el funcionamiento de una tienda en línea, ya que almacena y gestiona información crítica como productos, clientes, pedidos y pagos. A continuación, se detallan los aspectos esenciales a considerar:

1. **Componentes esenciales de la base de datos:** Una estructura bien diseñada debe incluir las siguientes tablas principales:
    - **Clientes:** Contiene información personal, datos de contacto y preferencias de compra.
    - **Productos:** Incluye descripciones, precios, imágenes y niveles de inventario.

- **Pedidos:** Registra detalles de las compras, fechas, estados y métodos de pago.
- **Artículos de pedido:** Relaciona productos específicos con pedidos, indicando cantidades y precios.
- **Métodos de pago y envío:** Almacena las opciones disponibles y sus configuraciones.
- **Inventario:** Monitorea la disponibilidad de productos en tiempo real.

Una base de datos bien estructurada facilita la gestión eficiente y escalable de la tienda en línea.

2. **Diseño y normalización del esquema**: Es crucial definir claramente las relaciones entre las tablas para evitar redundancias y asegurar la integridad de los datos. La normalización ayuda a organizar la base de datos de manera que se minimicen las duplicaciones y se mantenga la coherencia de la información.

3. **Elección del sistema de gestión de bases de datos (DBMS):** La selección del DBMS debe basarse en las necesidades específicas del negocio:
   - Relacionales (SQL): MySQL y PostgreSQL son opciones robustas para datos estructurados y transacciones complejas.
   - NoSQL: MongoDB y Cassandra ofrecen flexibilidad para manejar datos no estructurados y escalar horizontalmente.

La elección dependerá de factores como el tipo de datos que se van a manejar, la escalabilidad requerida y la experiencia del equipo técnico.

4. **Escalabilidad y rendimiento:** Es esencial que la base de datos pueda adaptarse al crecimiento del negocio. Esto implica considerar soluciones que permitan escalar vertical u horizontalmente y que mantengan un rendimiento óptimo a medida que aumenta la carga de trabajo.

5. **Seguridad y cumplimiento**: La protección de los datos sensibles es una prioridad. Se deben implementar medidas como cifrado de datos, control de accesos y auditorías regulares para cumplir con normativas como el GDPR en el caso de la Unión Europea y garantizar la confianza de los clientes.

6. **Integración con otras herramientas**: La base de datos debe ser compatible con otras soluciones utilizadas en la tienda, como sistemas de gestión de

relaciones con clientes (CRM), plataformas de marketing y herramientas de análisis. Esto facilita una operación más fluida y una mejor toma de decisiones basada en datos.

7. **Mantenimiento y respaldo**: Es fundamental establecer procedimientos para el mantenimiento regular de la base de datos, incluyendo copias de seguridad automáticas y monitoreo continuo, para prevenir pérdidas de datos y asegurar la continuidad del negocio.

Sistemas de pago

Dentro de los sistemas de pago existen varias formas para realizar las transacciones, aunque es verdad que se realizan de alguna plataforma electrónica no todos tienen el mismo procedimiento. A nivel global las tarjetas de crédito, débito y monederos digitales son las formas más dominantes en el sin embargo existen las transferencias bancarias y el efectivo aún siguen siendo métodos de pago, los métodos de pago que existen serían los siguientes:

1. **Tarjetas de crédito y débito**
   - La tarjeta de crédito y débito son la forma más común de hacer pagos en el mercado actual, proveen rapidez y sencillez al hacer pagos aparte de proveer seguridad de fraude.
2. **Monederos digitales**
   - Los monederos tipo PayPal, Apple Play, y Google Play han sido los métodos alternativos que los pagos se han estado realizando al igual que las tarjetas de crédito y débito tienen la credibilidad para mantener tu dinero a salvo, en lugares como Estados Unidos este método de pago está siendo igual de usado que las tarjetas de crédito.
3. **Transferencias bancarias**
   - Este método se realiza enviando el monto requerido de una cuenta bancaria hacia la cuenta bancaria de la empresa, es un método lento a diferencia de los otros 2 métodos sin embargo son bastante populares en lugares de Europa y Asia, a diferencia de los métodos anteriores las transferencias pueden ser utilizadas internacionalmente.
4. **Pagos móviles**

- Los pagos móviles son bastante similares a los monederos digitales ya que van en conjunto sin embargo hay que aclarar que los pagos móviles como el nombre lo dice se limita a teléfonos, iPad etc., mientras que los monederos pueden ser utilizados por computadoras, los monederos utilizan tokens y los teléfonos utilizan métodos como QR o NFC

5. **Criptomonedas**
    - A pesar de tener poca seguridad sobre este método de pago sigue siendo utilizado por varios comercios especialmente minoristas

Seguridad

La seguridad dentro de los comercios electrónico abarca todo lo que es la ciberseguridad que garantizan seguridad a la hora de manejar información delicada como datos personales de una persona, números de una transacción en específico, y el proceso de pagos de ellos, por lo que la ciberseguridad es un elemento esencial a la hora de crear un comercio electrónico, sin embargo, porque es importante la ciberseguridad dentro de los comercios

- **Importancia de la ciberseguridad en los comercios electrónicos**

  Dentro del mundo criminal los ciberataques han sido una forma rentable de hacer dinero ya sea por extracción de información de una empresa o de alguien en específico elementos que como empresa si se descuida afecta la confiabilidad de un negocio, por lo que tener una buena forma de proteger esta información hace que el público pueda confiar más en una empresa

- **Recomendaciones de seguridad que se pueden implementar**

  Podemos mencionar varias prácticas como mantener un software actualizado, realizar copias de seguridad, brindar seguridad en los medios de pago, obtener certificado de SSL, solicitar CVV y AVS esta sería una de las prácticas que se pueden utilizar dentro de un comercio electrónico.

Desarrollo de software seguro de OWASP

OWASP (Open Worldwide Aplication Security Project) es una comunidad abierta dedicada a permitir que las organizaciones diseñen, desarrollen,

adquieran, operen y mantengan software para aplicaciones seguras en las que se pueda confiar. Sus programas incluyen proyectos de software de código abierto dirigidos por la comunidad y conferencias locales y globales, que involucran cientos de capítulos en todo el mundo con decenas de miles de miembros Es una comunidad abierta dedicada a permitir que las organizaciones diseñen, desarrollen, adquieran, operen y mantengan software para aplicaciones seguras en las que se pueda confiar. Sus programas incluyen proyectos de software de código abierto dirigidos por la comunidad y conferencias locales y globales, que involucran cientos de capítulos en todo el mundo con decenas de miles de miembros.

El Top 10 de OWASP

Es un informe actualizado de forma regular que subraya las preocupaciones de seguridad en el caso de la seguridad de las aplicaciones web, centrándose en los 10 riesgos más vitales. El informe es confeccionado por un equipo de expertos en seguridad de todo el mundo.

1. Pérdida de control de acceso

El control de acceso gestiona quién puede acceder a la información o funcionalidad de un sistema. Si no funciona correctamente, los atacantes pueden eludir la autorización y realizar acciones como usuarios privilegiados. Un ejemplo sería una aplicación web que permita a un usuario cambiar de cuenta solo modificando una URL, sin más verificaciones. Para asegurar el control de acceso, es importante usar tokens de autorización y establecer medidas estrictas sobre ellos.

2. Fallos criptográficos

Si las aplicaciones web no encriptan datos confidenciales como contraseñas o información financiera, los atacantes pueden acceder a ellos y usarlos con fines maliciosos, incluso mediante ataques en ruta (interceptando la comunicación).

3. Inyección

Los ataques de inyección ocurren cuando se envían datos maliciosos a través de formularios u otras entradas, y el sistema los interpreta como código. Un ejemplo común es la inyección SQL, donde un atacante inserta código SQL en

lugar de datos normales, logrando que el sistema lo ejecute si no está bien protegido.

4. Diseño no seguro

El diseño no seguro abarca vulnerabilidades presentes desde la arquitectura de una aplicación, sin importar su implementación. Un ejemplo es el uso de preguntas de seguridad para recuperar contraseñas, ya que pueden ser fáciles de adivinar. Para prevenir esto, se recomienda aplicar modelado de amenazas antes de desarrollar la aplicación.

5. Mala configuración de la seguridad

La desconfiguración de seguridad es una de las vulnerabilidades más comunes y suele deberse a configuraciones por defecto o mensajes de error demasiado detallados. Para evitarla, se recomienda eliminar funciones innecesarias y usar mensajes de error generales. También se aconseja usar formatos de datos más simples como JSON y desactivar entidades externas en XML para prevenir ataques XEE

6. Componentes vulnerables y obsoletos

El uso de bibliotecas y marcos facilita el desarrollo web, pero puede introducir vulnerabilidades si no se actualizan o provienen de fuentes no confiables. Se recomienda eliminar los componentes no usados y asegurarse de usar versiones actualizadas y seguras.

7. Fallos de identificación y autenticación

Las fallas en la autenticación pueden permitir el acceso no autorizado a cuentas, incluso de administradores. Para prevenirlo, se recomienda usar autenticación en dos pasos (2FA) y limitar los intentos de inicio de sesión.

8. Fallos de integridad de software y datos

Muchas aplicaciones dependen de fuentes externas y pueden ser vulnerables si no verifican la integridad de sus actualizaciones. Esto incluye riesgos como actualizaciones maliciosas o deserialización insegura, que pueden causar ataques graves. Se recomienda usar firmas digitales, revisar la cadena de suministro y proteger los procesos de desarrollo.

9. Fallos de registro y supervisión de seguridad

Muchas aplicaciones web no detectan a tiempo las fugas de datos, lo que permite a los atacantes actuar durante meses sin ser descubiertos. OWASP recomienda implementar registros, monitoreo y planes de respuesta a incidentes para reaccionar rápidamente ante ataques.

10. Falsificación de solicitudes del lado del servidor

La falsificación de solicitud del lado del servidor (SSRF) es un ataque que engaña al servidor para acceder a recursos restringidos y obtener información confidencial.

Conclusiones

Madelaine Arosemena: Este estudio me permitió comprender no solo los elementos básicos para desarrollar un sitio web de comercio electrónico, como el hosting, dominio, pasarelas de pago y base de datos, sino también la importancia crítica de la seguridad web. Aprendí que el Top 10 de OWASP es una guía esencial para identificar y mitigar las amenazas más comunes, como las inyecciones SQL, fallas de autenticación, exposición de datos sensibles o configuración incorrecta de seguridad. Estos conceptos son clave para proteger tanto la información del usuario como la integridad del sistema. Como futura desarrolladora, aplicar estas buenas prácticas desde el inicio de un proyecto web es fundamental para garantizar sitios seguros y confiables.

Javier Hernández: Esta investigación me permitió comprender la importancia de tomar decisiones estratégicas en aspectos técnicos clave para el desarrollo de un comercio electrónico. Aprendí que la elección adecuada de un proveedor de servicios de internet influye directamente en la disponibilidad y el rendimiento del sitio. También entendí que una base de datos bien estructurada es fundamental para la gestión eficiente de la información. Además, pude identificar los criterios esenciales para seleccionar sistemas de pago seguros y funcionales, y profundicé en las prácticas de seguridad necesarias para proteger la plataforma, destacando los principios de OWASP como una guía esencial para el desarrollo de software seguro.

Joel Castillo: Podemos concluir en esta investigación de la importancia de tener una seguridad sólida para un negocio comercial, también se demostró las buenas prácticas para poder tener un ambiente de seguro sano al igual que se dio recomendaciones sobre que destaca una página confiable y como puedo afectar a la imagen el nivel de seguridad, se estuvo abarcando los métodos de pago actuales de más comunes hasta los más poco utilizados dentro del mercado, algo que principalmente se debe de tomar en cuenta a la hora de hacer un negocio.

Referencias bibliográficas

1. *¿Cuáles son los mejores proveedores de servicios de Internet para empresas de comercio electrónico?* (n.d.). https://www.linkedin.com/advice/0/what-best-internet-service-providers-e-commerce-bhqec?lang=es&originalSubdomain=es
2. Ladonorte. (2024, June 26). *¿Cómo elegir al mejor proveedor de servicio de internet para tu empresa?* Netline. https://www.netline.net/como-elegir-al-mejor-proveedor-de-servicio-de-internet-para-tu-empresa/
3. Wolf Agencia de marketing digital. (2025, February 2). *Base de datos eficiente para ecommerce que impulsa el rendimiento y la gestión de ventas*. Wolf Agencia De Marketing Digital. https://wolfagenciademarketing.com/base-de-datos-para-ecommerce/?utm_source=chatgpt.com
4. Bengochea, D. (2022, August 3). *Cómo Crear una Base de Datos de una Tienda Online*. Outvio. https://outvio.com/es/blog/base-de-datos-tienda-online/?utm_source=chatgpt.com
5. Lureo Digital. (2025, February 1). *Cómo crear una base de datos efectiva para tu tienda online: 5 tips esenciales*. Lureo Digital: Tu Socio Estratégico En El Mundo Digital. https://lureodigital.com/como-crear-una-base-de-datos-efectiva-para-tu-tienda-online-5-tips-esenciales/?utm_source=chatgpt.com
6. *Métodos de pago de e-commerce: instrucciones para elegir uno | Stripe*. (2025, 23 enero). https://stripe.com/es/resources/more/ecommerce-payment-methods#:~:text=Las%20tarjetas%20de%20cr%C3%A9dito%20y,de%20forma%20r%C3%A1pida%20y%20c%C3%B3moda.&text=Los%20monederos%20digitales%2C%20como%20PayPal,cada%20vez%20son%20m%C3%A1s%20populares.

7. *Seguridad en el Comercio Electrónico: Medidas e Importancia*. (2023, 2 agosto). https://www.conekta.com/blog/seguridad-comercio-electronico
8. *¿Qué es Open Worldwide Application Security Project (OWASP)?* (s. f.). F5, Inc. https://www.f5.com/es_es/glossary/owasp
9. *(S/f). Cloudflare.com. Recuperado el 19 de abril de 2025, de https://www.cloudflare.com/es-es/learning/security/threats/owasp-top-10/*