UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS

DESARROLLO DE SOFTWARE IX

PRESENTACIÓN #1

COMERCIO ELECTRÓNICO:

EQUIPO #4

PROFESOR:

Erick Agrazal

INTEGRANTE(S):

John Grant | 8-983-1525

Víctor Rodríguez | 20-70-7414

AÑO

2025

CONTENIDO

1. ¿Qué es un ISP?

Un ISP, siendo las siglas de “Internet Server Provider” o “Proveedor de servicios de internet”, son entes o compañías que se encargan de brindar conexión a internet a sus usuarios. Lo hacen por medio de cable coaxial, fibra óptica o satélite.

La conexión a internet es fundamental para el funcionamiento de un comercio electrónico, es lo que despliega la interfaz y todas las operaciones que trascurren en ella. Por ello, la estabilidad que brinda un ISP debe ser adecuada para que todo pueda fluir de forma correcta.

En Panamá existen muchos ISP, de los cuales los más conocidos son:

- Más Móvil
- Tigo
- Packet Hub S.A.
- Cyberzone S.A.
- Universidad Tecnológica de Panamá

2. Como elegir y Trabajar con un ISP

Para elegir correctamente un ISP enfocado a manejar un Comercio Electrónico debemos considerar un servicio de calidad, veloz, accesible y estable para que todos los procesos fluyan de manera óptima. La escalabilidad del servicio debe ser apto para el tipo de comercio que se maneja y adaptarse a los cambios en su mercado, así como una buena cobertura para que los procesos que se almacenan en servicios externos lleguen sin ningún tipo de retraso.

La seguridad y la respuesta a caídas de conexión que ofrece un ISP también en muy importante ya que al ser un sitio que maneja transacciones, debe haber prioridad máxima

a garantizar una navegación fluida para los usuarios. Un sitio con frecuentes caídas del servidor o con poca seguridad por parte de la red minimiza la confianza de los usuarios y afecta a su regreso para futuras necesidades.

3. Consideraciones en la Base de Datos

¿Qué base de datos escoger para un e-commerce?

Se suele subestimar la elección de la base de datos, han sido varias las ocasiones en las que, en un trabajo de equipo, el grupo no le da mayor importancia a la base de datos, más que guarde los datos que se necesitan para desarrollar el proyecto, cuando el diseño de esta es fundamental para el rendimiento, escalabilidad y confiabilidad del sistema.

Existen diferentes factores a considerar, un e-commerce es suceptible a experimentar un rápido crecimiento de usuarios y tráfico, por lo que la solución debe ser **escalable.** La **eficiencia e integridad de los datos** son características esenciales para los e-commerce, la cantidad de transacciones con información confidencial obligan, prácticamente, al desarrollador a evaluar qué tan bien la base de datos admite las **propiedades ACID**, de la que hablaremos más adelante.

Se deben considerar los **tipos de datos** que la plataforma va a recopilar y almacenar, de la misma manera, a nivel de seguridad, deben existir diferentes mecanismos que aseguren la información confidencial, como cifrado de datos, autenticación de usuarios y/o control de acceso.

Pricipios ACID

ACID es un acrónimo de las cuatro propiedades principales de una base de datos: atomicidad, coherencia, aislamiento y durabilidad. A pesar de que se suele asociar a bases de datos relacionales, una base de dato NoSQL también puede seguir las reglas ACID que se compone de:

- Atomicidad: Con la atomicidad, la base de datos revierte todas las transacciones cuando una falla, para que los datos se mantengan homogéneos y eviten la corrupción
- Coherencia: significa que los datos pueden predecirse, lo que quiere decir que si se extraen datos para un registro en concreto, obtendrá un resultado esperado
- Aislamiento: Las lecturas sucias y las escrituras sucias se producen cuando un usuario ejecuta una consulta en el momento específico en que la base de datos también realiza cambios en un valor. Por ejemplo, si quiere saber el total de todos los pedidos del mes, puede obtener un resultado incorrecto si lee los datos en el momento en que se actualiza el total de un pedido.

- Durabilidad: Tanto las bases de datos estructuradas como las no estructuradas deben almacenar los datos de manera constante y permanente después de que se complete una transacción, incluso si hay un fallo del sistema.

Bases de datos relacionales

De acuerdo con Rendón (2019) las bases de datos relacionales s*on una colección de elementos de datos organizados en un conjunto de tablas formalmente descritas, desde donde se puede acceder a los datos o volver a montarlos de muchas maneras diferentes sin tener que reorganizar las tablas de la base.* ***La interfaz estándar de programa de usuario y aplicación a una base de datos relacional es el Lenguaje de Consultas Estructuradas (SQL)****. (A. Rendón. 2019).*

Bases de datos no relacionales

Siguiendo el hilo de Rendón, las bases de datos no relacionales son utilizadas, por lo general, para modelos de datos específicos y tienen esquemas flexibles para crear apps modernas. Son, a nivel de funcionalidad y en rendimiento a escala, fáciles de desarrollar. Usan una variedad de modelos de datos que incluyen documentos, gráficos, clave-valor, en memoria y búsqueda.

Las bases de datos NoSQL son las que no tienen un identificador que sirva de relación entre un conjunto de datos y otros, a diferencia de las SQL DB.

Diferencias

Para entender las diferencias, imaginemos que un edificio de la ciudad de Panamá sigue determinados estándares de construcción y que, si algún residente decide hacer un cambio, estaría afectando directamente la estructura (modelo) lo que lo haría incompatible con el resto de los apartamentos y obligaría a modificar el hogar de los vecinos.

Por otro lado, imaginemos que, en Darién, los indígenas construyen casas a su antojo, sin seguir un determinado patrón o modelo, construyendo a su gusto, digamos. Si alguno decidiera hacer un cambio a su hogar, no pasaría absolutamente nada con el resto de las viviendas, todas seguirían funcionando sin problema.

En las bases de datos no relacionales los datos se pueden almacenar de cualquier manera:

- Documento (MongoDB),
- Clave – Valor (Redis),
- Gráfico (Neo4j),

- Columna (Cassandra)

4. **Sistemas de pago:**

En Panamá, las estadísticas señalan que el comercio electrónico en Panamá creció aproximadamente un 40% durante pandemia y representó, en el 2022, el 11% de las ventas minoristas totales en Panamá.

Pero ¿cómo llegamos a esto? Para que esta actividad sea exitosa es imprescindible contar con un sistema de pago seguro y confiable y, entonces, entran en juego las pasarelas de pago.

Las pasarelas de pago autorizan y procesan los pagos con tarjetas de crédito o débito para pagos en línea y puede ser proporcionada por un banco, un proveedor de servicios de pago o un proveedor de servicios de aplicaciones de comercio electrónico.

En Panamá existen varias opciones al momento de elegir una pasarela de pago, en el siguiente cuadro podremos ver una comparación entre las principales del país. A continuación alguna de ellas:

Pasarela	Requisitos principales	Integración
BAC Credomatic	-Sitio web con carrito de compras. -Políticas de entrega, cancelación, devoluciones, privacidad, T&C. Logo de Visa, MC, AmEx	Plugin de tercero para WooCommerce. (Costo adicional)
Credicorp Bank	- Propuesta firmada. - Solicitud e-commerce firmada. - Aviso de operaciones. - Identificación y recibo de servicio público	Cargo único de integración + planes de pago
Yappy	**Personal:** mayor de edad, aviso de operación (si extranjero), cuenta en BG, redes sociales, Tarjeta Clave o Visa débito	Botón de pago web / QR estático o dinámico / directorio Yappy

	Comercial: cuenta y banca en línea comercial en BG	
Wompi (Banistmo)	- Pago inicial de US$ 50	API o link de pago

5. Seguridad en un Comercio Electrónico

De acuerdo con el equipo editorial Conekta, la seguridad en el comercio electrónico abarca todas las medidas de ciberseguridad que garantizan protección en cualquier transacción de compraventa a través de Internet. Esto implica seguir pautas y normas aceptadas a nivel mundial para permitir que las personas puedan comprar y vender de forma segura en línea.

Existen una serie de principios que se deben cumplir para que un comercio electrónico pueda considerarse mínimamente seguro.

- Privacidad: implica que el comercio electrónico debe evitar cualquier actividad que lleve a compartir datos de los clientes con terceras personas no autorizadas.
- Integridad: los datos o información que un cliente comparta para una compra en línea deben permanecer sin modificarse ni alterarse.
- Autenticación: El principio de autenticación establece que tanto el vendedor como el comprador sean reales y verificables. Es decir, son quienes dicen ser.
- No repudio: el no repudio es un principio legal que obliga tanto al vendedor como al comprador a aceptar y darle seguimiento a la transacción que iniciaron.

5.1 Desarrollo de Software Seguro de OWASP

OWASP (Open web application security project) es una ONG que promueve la seguridad en el desarrollo de software. Su objetivo principal es ayudar a desarrolladores a construir aplicaciones seguras a través de guías, herramientas y buenas prácticas. Alguno de los principios fundamentales de la seguridad de aplicaciones son:

- Modelo de madurez de seguridad de software (SAMM): proporciona contexto para el alcance de la seguridad del software y fundamentos de las buenas prácticas de seguridad:
    - Gobernanza
    - Diseño
    - Implementación
    - Verificación
    - Operaciones
- Tríada CIA: La seguridad consiste en controlar quién puede interactuar con la información, qué pueden hacer con ella y cuándo pueden interactuar con ella. Estas características de seguridad se pueden describir utilizando la tríada CIA. CIA significa confidencialidad, integridad y disponibilidad.
- Confidencialidad: significa protección de los datos contra la divulgación no autorizada.
- Integridad: La integridad consiste en proteger los datos contra modificaciones no autorizadas o garantizar la confiabilidad de los datos.
- Disponibilidad: garantiza la presencia de información o recursos.
- Tríada AAA: La tríada de la CIA a menudo se amplía con Autenticación, Autorización y Auditoría
- Autenticación: consiste en confirmar la identidad de la entidad que desea interactuar con un sistema seguro.
- Autorización: consiste en especificar derechos de acceso a recursos seguros
- Auditoría: consiste en realizar un seguimiento de lso eventos a nivel de implementación.

Top 10 de riesgos de seguridad en aplicaciones web.

- Control de Acceso Roto (Broken Access Control): permite a usuarios no autorizados acceder a funciones o datos restringidos.
- Fallos Criptográficos (Cryptographic Failures): problemas en la protección de datos sensibles debido a una criptografía inadecuada.
- Inyecciones (Injection): inserción de código malicioso (como SQL, NoSQL, OS, LDAP) en una aplicación.

- Diseño Inseguro (Insecure Design): deficiencias en el diseño de la aplicación que permiten vulnerabilidades.
- Configuración de Seguridad Incorrecta (Security Misconfiguration): configuraciones predeterminadas inseguras o mal configuradas en servidores, bases de datos, etc.
- Componentes Vulnerables y Desactualizados (Vulnerable and Outdated Components): uso de bibliotecas o componentes con vulnerabilidades conocidas.
- Fallos de Identificación y Autenticación (Identification and Authentication Failures): debilidades en la autenticación de usuarios, como contraseñas débiles o tokens inseguros.
- Fallos en la Integridad del Software y de los Datos (Software and Data Integrity Failures): falta de verificación en actualizaciones de software o datos críticos.
- Fallos en el Registro y Monitoreo de la Seguridad (Security Logging and Monitoring Failures): ausencia de registros y monitoreo adecuados para detectar y responder a incidentes.
- Falsificación de Solicitudes del Lado del Servidor (Server-Side Request Forgery - SSRF): la aplicación puede ser inducida a realizar solicitudes a destinos no deseados.

BIBLIOGRAFÍA

Rendón, Y. A. (2019, 28 de mayo). *Bases de datos relacionales vs. no relacionales*. Pragma. https://www.pragma.com.co/academia/lecciones/bases-de-datos-relacionales-vs.-no-relacionales pragma.com.co+1pragma.com.co+1

AppMaster. (2023, 28 de septiembre). *Seleccionar la base de datos ideal para su tienda de comercio electrónico*. https://appmaster.

Pure Storage. (2023, 28 de septiembre). *¿Qué es la base de datos ACID?*. https://www.purestorage.com/es/knowledge/what-is-database-acid.html

Jootser Technologies. (2023, 4 de julio). *Pasarelas de pago para e-commerce en Panamá: Guía completa*. https://jootser.com/pasarelas-de-pago-para-e-commerce-en-panama/

Equipo Editorial Conekta. (2023, 2 de febrero). *Seguridad en el comercio electrónico: Medidas e importancia*. Conekta. https://www.conekta.com/blog/seguridad-comercio-electronico conekta.com

***Internet Service Providers in Panama*. (s/f). Db-ip.com. Recuperado el 17 de abril de 2025, de** https://db-ip.com/country/PA

***¿Qué Es un ISP? Todo Lo Que Necesitas Saber*. (2022, junio 16). Kinsta®; Kinsta.** https://kinsta.com/es/base-de-conocimiento/que-es-un-isp/

CONCLUSIONES

John Grant: Esta experiencia me hizo conocer términos y conceptos ligados a mi profesión que no tenía tan claro por lo poco que se manejaban en otras asignaturas, pero ahora que nos enfocamos de lleno en el comercio electrónico, el conocimiento de ellos es muy necesario debido a que forman parte de las claves para un sistema eficiente. Desde los ISP, los sistemas de pago y la seguridad son elementos que de ahora en adelante serán indispensables en mi carrera como programador.

Víctor Rodríguez: Desarrollar esta actividad me ha aclarado la diferencia que existe entre las bases de datos sql y noSql y la dependencia que existe en el rendimiento, seguridad y autenticidad con respecto al análisis previo del sistema. Es importantisimo poder tener la capacidad de determinar qué tecnología se amolda mejor al objetivo que queremos alcanzar.

De la misma manera, logré tener un entendimiento básico de OWASP y las consecuencias de mantener un desarrollo de software seguro.