Universidad Nacional de Trujillo

Ética para profesionales en Informática

III UNIDAD

COMERCIO ELECTRONICO

Apellidos y nombres:

……..

2024

Comercio Electrónico

1. ¿Qué es el Comercio Electrónico?

.....
.....
.....

Características principales:

- Se realiza en plataformas digitales.
- Utiliza métodos de pago electrónicos (tarjetas, transferencias, billeteras digitales).
- Puede incluir bienes físicos (ropa, libros) o servicios digitales (software, cursos en línea).

2. Historia del Comercio Electrónico

Origen (1970-1990):

- **1970s:** Comienza con sistemas como **Electronic Data Interchange (EDI)**, que permitían a las empresas intercambiar documentos comerciales de manera electrónica.
- **1980s:** Nace el concepto de compras en línea. Empresas grandes comienzan a experimentar con sistemas de transacciones digitales.
- **1990:** El nacimiento de Internet marcó un punto de inflexión, al permitir el acceso masivo a las transacciones electrónicas.

Crecimiento (1990-2000):

- **1991:** Se abre Internet al uso comercial.
- **1994:** Aparece **Amazon**, inicialmente como una librería en línea.
- **1995:** Nace **eBay**, introduciendo las subastas en línea.
- **Finales de los 90:** Empresas como **PayPal** surgen para facilitar pagos electrónicos, impulsando aún más el comercio electrónico.

Consolidación (2000-2020):

- **2000s:** Las plataformas digitales comienzan a optimizar la experiencia del usuario. Nace el concepto de **marketplaces**.
- **2010s:** La explosión de los **smartphones** impulsa las compras a través de aplicaciones móviles.
- **2020:** La pandemia de COVID-19 acelera el crecimiento del comercio electrónico, aumentando las compras en línea.

Actualidad (2020 en adelante):

- La **inteligencia artificial** y los **chatbots** están transformando la experiencia de compra.
- Se han popularizado los métodos de pago digitales como **billeteras electrónicas** (Google Pay, Apple Pay) y las **criptomonedas**.
- La logística ha evolucionado con tecnologías como drones y almacenes inteligentes.

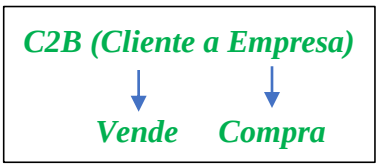
Actividad 1:

Elabore una Línea de Tiempo de la Historia del Comercio Electrónico

3. Modalidades de Comercio Electrónico

La matriz **3x3** representa las interacciones entre **clientes (C)**, **empresas (B)** y **gobierno (G)** en el comercio electrónico. Cada combinación define una modalidad de interacción. A continuación, se describen las **9 modalidades** con ejemplos.

Categorías	Cliente (C)	Empresa (B)	Gobierno (G)
Cliente (C)	C2C: Cliente a Cliente	C2B: Cliente a Empresa	C2G: Cliente a Gobierno
Empresa (B)	B2C: Empresa a Cliente	B2B: Empresa a Empresa	B2G: Empresa a Gobierno
Gobierno (G)	G2C: Gobierno a Cliente	G2B: Gobierno a Empresa	G2G: Gobierno a Gobierno



1. C2C (Cliente a Cliente)

Los consumidores venden productos o servicios entre ellos mediante plataformas digitales.

- Ejemplo: Venta de artículos usados en **eBay** o **Mercado Libre**.

2. C2B (Cliente a Empresa)

Los consumidores ofrecen servicios o productos que las empresas compran.

- Ejemplo: Un influencer que promociona una marca en Instagram por una tarifa.

3. C2G (Cliente a Gobierno)

Los ciudadanos realizan venta de un bien o servicio al gobierno en línea.

- Un profesional independiente diseña y vende material gráfico para una campaña del gobierno de manera digital.

4. B2C (Empresa a Cliente)

Las empresas venden productos o servicios directamente al consumidor final.

- Ejemplo: Comprar productos en **Amazon** o servicios en **Netflix**.

5. B2B (Empresa a Empresa)

Transacciones entre empresas, como la compra de insumos o servicios especializados.

- Ejemplo: **Salesforce**, que provee software a otras empresas.

6. B2G (Empresa a Gobierno)

Las empresas proporcionan productos o servicios al gobierno.

- Ejemplo: Una empresa que vende software de gestión al gobierno a través de una licitación.

7. G2C (Gobierno a Cliente)

El gobierno ofrece servicios directamente a los ciudadanos en línea.

- Ejemplo: Solicitud de certificados de nacimiento en línea mediante **RENIEC** en Perú.

8. G2B (Gobierno a Empresa)

El gobierno interactúa con empresas para regulaciones, licitaciones o servicios.

- Ejemplo Empresas adquieren licencias de funcionamiento o permisos operativos a través de portales gubernamentales.

9. G2G (Gobierno a Gobierno)

Intercambios entre entidades gubernamentales.

- Ejemplo: Un ministerio compartiendo información con otro mediante un sistema digital centralizado.

Actividad 2:

Casos simulados de las 9 modalidades

Cada caso describe una situación. Los estudiantes deben identificar a qué modalidad pertenece cada uno:

1. **Caso 1:** Juana vende sus zapatos usados a través de una publicación en Facebook Marketplace.

2. **Caso 2:** Una empresa de catering provee alimentos para los eventos oficiales del gobierno local.

3. **Caso 3:** Manuel paga sus impuestos prediales en el portal municipal.

4. **Caso 4:** María compra un curso de inglés en línea en una plataforma educativa.

5. **Caso 5:** Una compañía de transportes contrata a una empresa para comprar un sistema de rastreo de vehículos para optimizar sus rutas.

6. **Caso 6:** El Ministerio de Educación comparte datos de estudiantes con el Ministerio de Salud para campañas de vacunación.

7. **Caso 7:** Un diseñador gráfico independiente vende un logotipo a una empresa emergente en Fiverr.

8. **Caso 8:** Un ciudadano solicita un permiso de construcción en el portal de urbanismo de su ciudad.

9. **Caso 9:** Un fabricante de computadoras compra componentes electrónicos a un proveedor en China.

Actividad 3:

Ejemplo de Compra:

A. Describe una compra que hayas realizado mediante comercio electrónico.

Incluye detalles como el producto o servicio adquirido, la plataforma utilizada (por ejemplo, Amazon, Mercado Libre, etc.), y el proceso seguido para concretar la compra.

……

……

……

……

Determinación de Modalidad:……..

Responde las siguientes preguntas relacionadas con tu experiencia de compra:

¿Por qué decidiste realizar la compra por comercio electrónico en lugar de en una tienda física?

……

……

¿Cómo calificas tu experiencia en términos de tiempo, costo y facilidad de uso?

……

……

Reflexión Final:

Reflexiona sobre los beneficios y desventajas que encontraste al comprar a través de comercio electrónico.

……

……

……

……

Para el cliente

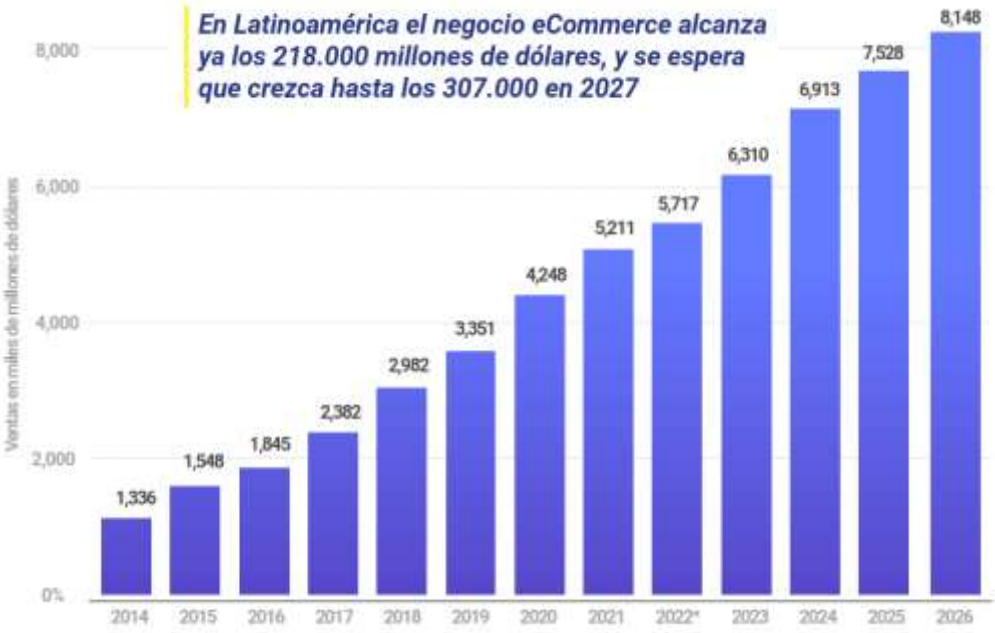
Ventajas	***Desventajas***
……	……
……	……
……	……
……	……
……	……
……	……
……	……
……	……
……	……
……	……

Para la empresa

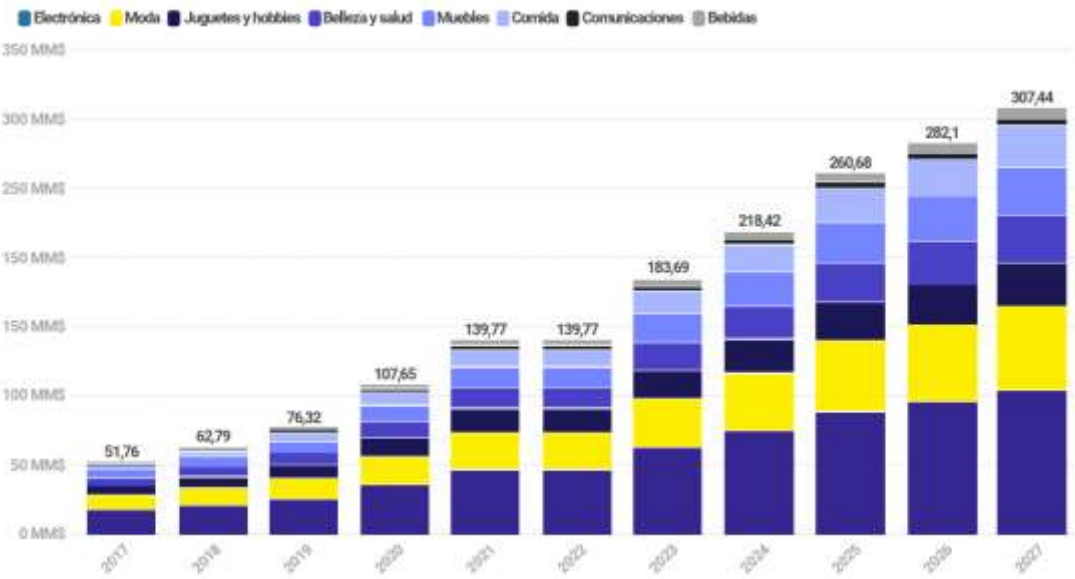
Ventajas	***Desventajas***
…… …… …… …… …… …… …… …… …… ……	…… …… …… …… …… …… …… …… …… ……

4. Estadísticas del comercio electrónico

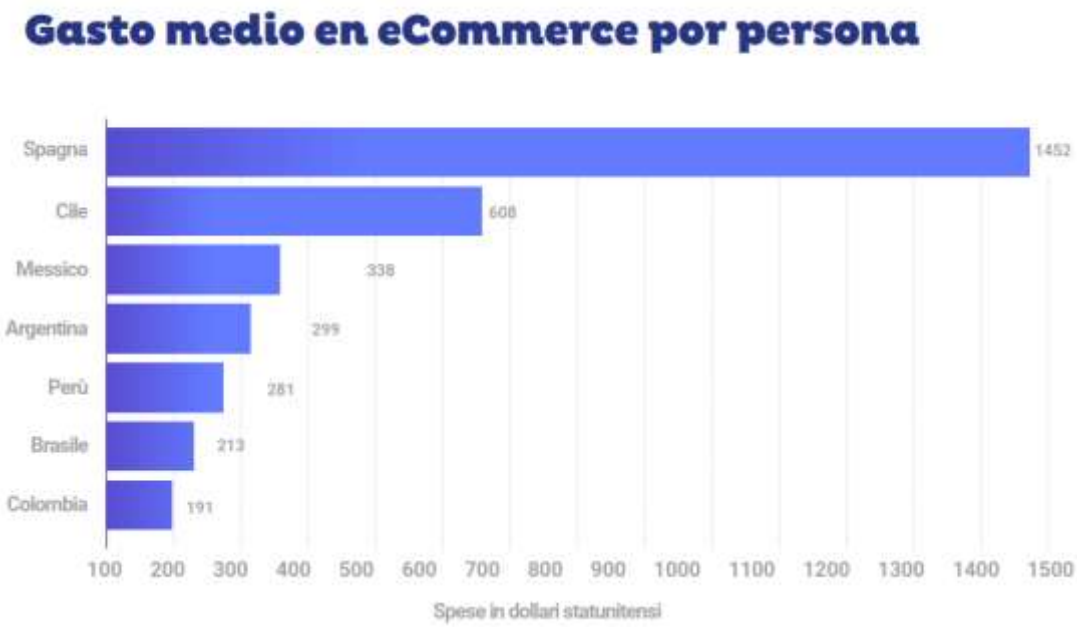
Análisis/comentario……
……
……



Análisis/comentario……
……
……



Análisis/comentario……
……
……



Análisis/comentario……
……
……

Principales Delitos y Estafas en el Comercio Electrónico

El comercio electrónico ha revolucionado la economía global, ofreciendo accesibilidad y eficiencia tanto a empresas como a consumidores. Sin embargo, la misma tecnología que facilita estas transacciones ha abierto la puerta a una variedad de delitos cibernéticos y estafas que comprometen la seguridad, privacidad y confianza en las plataformas en línea. Este marco teórico analiza los principales delitos relacionados con el comercio electrónico, sus características, impacto ético y medidas de prevención.

1. Phishing

Definición:

El phishing es un método de estafa en el que los ciberdelincuentes envían mensajes fraudulentos diseñados para parecer legítimos, con el objetivo de engañar a las víctimas para que proporcionen información confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios.

Características:

- Uso de correos electrónicos o sitios web falsos que imitan entidades legítimas.
- Solicitudes urgentes para "verificar" cuentas o información.

Impacto:

- Compromete la confianza en las plataformas digitales.
- Explotación de la vulnerabilidad del usuario.

Ejemplo: Un correo que simula ser de una plataforma como Amazon, solicitando datos personales para desbloquear una cuenta.

2. Robo de Identidad

Definición:

El robo de identidad ocurre cuando alguien utiliza información personal de otro individuo sin su permiso, generalmente para realizar transacciones financieras o acceder a servicios.

Características:

- Obtención de datos mediante hackeos, phishing o malware.
- Uso indebido de la identidad para cometer fraudes.

Impacto:

- Perjuicio a la reputación y finanzas de las víctimas.
- Violación de los derechos individuales y la privacidad.

Ejemplo: Un ciberdelincuente accede a los datos de una tarjeta de crédito y realiza compras en línea.

3. Fraude en los Pagos

Definición:

El fraude en los pagos incluye el uso no autorizado de tarjetas de crédito o débito, devoluciones fraudulentas, y suplantación de identidad en transacciones.

- Características:
- Transacciones realizadas sin el consentimiento del propietario de los métodos de pago.
- Estafas en las que se simulan devoluciones de dinero.

Impacto:

- Afecta tanto a los consumidores como a las empresas.
- Genera desconfianza en los sistemas de pago en línea.

Ejemplo: Un estafador utiliza un número de tarjeta robado para realizar una compra.

4. Malware en Portales Comerciales

Definición:

El malware es un software malicioso que se infiltra en sistemas para capturar información sensible de los usuarios, como datos financieros.

Características:

Infecta sistemas a través de sitios web vulnerables.

Puede incluir spyware, keyloggers y ransomware.

Impacto:

- Vulneración de la seguridad informática.
- Daño a la reputación de las empresas afectadas.

Ejemplo: Un sitio de comercio electrónico infectado recopila los datos de las tarjetas de sus usuarios.

5. Estafas de Productos Falsos

Definición:

Consiste en la venta de productos inexistentes o falsificados a través de plataformas de comercio electrónico.

Características:

- Ofrecen precios irresistibles para atraer víctimas.
- El producto nunca se entrega o no corresponde a lo anunciado.

Impacto:

- Perjuicio económico a los consumidores.
- Competencia desleal para las empresas legítimas.

Ejemplo: Un vendedor en un marketplace ofrece electrónicos a precios extremadamente bajos y nunca los envía.

6. Ataques de Denegación de Servicio (DDoS)

Definición:

Los ataques DDoS buscan colapsar plataformas en línea mediante un gran volumen de solicitudes falsas, impidiendo su funcionamiento.

Características:

- Paralizan sitios web de comercio electrónico.
- Se realizan con redes de bots automatizados.

Impacto:

- Perjuicio económico para las empresas.
- Afectación a miles de usuarios legítimos.

Ejemplo: Un marketplace sufre un ataque que lo deja fuera de servicio en días de alta demanda.

7. Ingeniería Social

Definición:

Es la manipulación psicológica para obtener información sensible, a menudo explotando la confianza de las víctimas.

Características:

- Se basa en interacciones humanas directas.
- Utiliza llamadas telefónicas o mensajes personalizados.

Impacto:

- Aprovecha la vulnerabilidad emocional de las personas.
- Daño irreparable a la confianza interpersonal.

Ejemplo: Un estafador convence a un cliente de que necesita proporcionar su contraseña para un supuesto soporte técnico.

Seguridad en el Comercio Electrónico

El comercio electrónico ha transformado las transacciones globales, brindando accesibilidad y conveniencia. Sin embargo, para garantizar su funcionamiento seguro y confiable, se deben implementar principios clave de seguridad. Estos principios protegen los datos, la identidad de los usuarios y la integridad de las transacciones. Entre ellos destacan el no repudio, la integridad, la confidencialidad y la autenticidad.

1. No Repudio

Definición:

El principio de no repudio asegura que ninguna de las partes involucradas en una transacción pueda negar haber participado en ella. Esto implica que tanto el emisor como el receptor no pueden rechazar la validez de un mensaje o transacción realizada.

Importancia en el Comercio Electrónico:

- Protege a las partes de disputas sobre transacciones completadas.
- Garantiza que los compradores y vendedores cumplan con sus compromisos.
- Utiliza mecanismos como firmas digitales y registros electrónicos.

2. Integridad

Definición:

La integridad asegura que los datos transmitidos o almacenados no han sido alterados de manera no autorizada. Esto es crucial para garantizar que la información sea precisa y confiable.

Importancia en el Comercio Electrónico:

- Protege los detalles de las transacciones, como precios, cantidades y métodos de pago.
- Evita el fraude asociado con la manipulación de datos durante la transmisión.

3. Confidencialidad

Definición:

La confidencialidad garantiza que la información sea accesible únicamente para las partes autorizadas, protegiendo los datos sensibles contra el acceso no autorizado.

Importancia en el Comercio Electrónico:

- Protege información personal y financiera de los usuarios, como números de tarjetas de crédito y datos de autenticación.
- Evita el robo de identidad y fraudes.

4. Autenticidad

Definición:

La autenticidad asegura que las partes involucradas en una transacción son quienes dicen ser. Verifica la identidad de usuarios, vendedores y plataformas.

Importancia en el Comercio Electrónico:

- Previene fraudes relacionados con la suplantación de identidad.
- Garantiza que los usuarios interactúen con sitios web legítimos.

Relación entre los Principios

Estos principios están interconectados para garantizar la seguridad global del comercio electrónico. Por ejemplo:

- La confidencialidad protege los datos sensibles, mientras que la integridad garantiza que no sean alterados.
- El no repudio y la autenticidad trabajan juntos para confirmar la identidad de las partes y evitar que nieguen su participación en transacciones.

Importancia de estos Principios en el Comercio Electrónico

Generar Confianza:

La seguridad fomenta la confianza entre consumidores y empresas.

Los usuarios confían más en plataformas que implementan medidas de seguridad visibles.

Proteger a las Partes Involucradas:

Los compradores y vendedores están protegidos contra fraudes y accesos no autorizados.

Los sistemas de seguridad minimizan las disputas relacionadas con transacciones.

Cumplimiento Legal y Normativo:

Muchas jurisdicciones exigen estándares de seguridad específicos para el comercio electrónico para proteger datos de tarjetas.

Fomento de la Innovación:

La seguridad permite el desarrollo de nuevas tecnologías, como monederos digitales y criptomonedas.

Conclusión

El comercio electrónico no puede existir sin medidas robustas de seguridad. Los principios de no repudio, integridad, confidencialidad y autenticidad son pilares esenciales que protegen a los usuarios y garantizan la transparencia y confiabilidad de las transacciones digitales. Los profesionales en informática deben diseñar sistemas que integren estos principios para promover una experiencia de comercio seguro y ético.

Actividad 4

Caso 1

Una persona compra una computadora en una tienda en línea confiable. Durante el proceso, introduce su dirección para el envío. Sin embargo, un atacante intercepta la comunicación entre la tienda y el proveedor de envíos, altera los datos, y la computadora se envía a una dirección diferente. La víctima nunca recibe el producto.

Principio Vulnerado: ……..

Impacto:

……

……

……

……

Caso 2

Un cliente compra un televisor en línea y paga con tarjeta de crédito. Después de recibir el producto, el cliente contacta al banco para negar la transacción, alegando que nunca realizó la compra. Como resultado, el vendedor enfrenta problemas para demostrar que el cliente realmente autorizó la operación.

Principio Vulnerado: ……..

Impacto:

……

……

……

……

Caso 3

Un usuario realiza una compra en un sitio web que no cuenta con cifrado. Los datos de su tarjeta de crédito son interceptados por un ciberdelincuente mediante un ataque cibernético. Posteriormente, el delincuente utiliza esta información para realizar compras no autorizadas.

Principio Vulnerado: ……..

Impacto:

……

……

……

……

Caso 4

Un usuario busca comprar un celular en línea y encuentra un sitio web con una oferta muy atractiva. El sitio parece legítimo y el usuario realiza el pago. Sin embargo, el sitio era una copia falsa de una tienda reconocida y el dinero termina en manos de los estafadores.

Principio Vulnerado: ……..

Impacto:

……

……

……

……

Actividad 5

Principios de Seguridad con Ética para una Tienda en Línea

Objetivo de la Actividad:

Diseñar principios de seguridad alineados con la ética profesional para garantizar la protección de los datos, la confianza de los clientes y la integridad de las transacciones en una tienda en línea.

Pasos para Realizar la Actividad

Contextualización:

Imagine que usted es el administrador de una tienda en línea que ofrece productos o servicios a través de plataformas digitales.

Reflexione sobre los principales riesgos de seguridad y los desafíos éticos que enfrenta una tienda de este tipo.

Creación de Principios de Seguridad:

Elabore 10 principios que su tienda en línea debe seguir para garantizar la seguridad y la ética en sus operaciones.

Cada principio debe incluir:

Una descripción breve de lo que establece.

Su relación con la seguridad digital y la ética profesional.

Ejemplo:

Confidencialidad de los Datos: "Nuestra tienda garantiza que los datos personales y financieros de los clientes serán almacenados de forma segura y utilizados exclusivamente para los fines autorizados, respetando su privacidad."