
Universidad
Tecmilenio®

Universidad Tecmilenio

Gestión avanzada de Tecnologías de la Información

Seguridad y pagos electrónicos

Introducción

La tecnología ha creado nuevos nichos de negocio en positivo y en negativo, es decir, por una parte, nos permite automatizar transacciones ahorrando tiempo, pero también nos hace vulnerables a ataques cibernéticos o robo de datos.
La seguridad se debe basar en tecnología, leyes y concientización a los usuarios de estos servicios, para no caer en trampas de hackers y saber cómo proteger nuestros datos personales, ya que, en la actualidad, cualquiera puede crear una página web e incluir imágenes de Mercado Pago, Visa, Mastercard o cualquier otra compañía que garantice las transacciones de pago.

Explicación

Amenazas de seguridad en línea

El tamaño total y las pérdidas ocasionadas por la **ciberdelincuencia** no quedan claros. Algunos datos indican que el 46% de los participantes de las encuestas detectaron haber tenido ataques cibernautas, sin embargo, muchas organizaciones deciden no denunciar los ataques por temor a perder la confianza de sus consumidores. La información robada se almacena en servidores de la economía informal.
Las amenazas más comunes en el ambiente de comercio electrónico son las siguientes:

Amenazas del comercio electrónico

- Código malicioso
- Programas potencialmente no deseados
- *Phishing* y robo de identidad
- *Hacking*
- Vandalismo cibernético
- Filtración de datos
- Fraude con tarjetas de crédito/robo
- *Spoofing (pharming)*
- Ataque de negación de servicio (DoS, por sus siglas en inglés, *Denial of Service*)
- Husmeador *(sniffing)*
- Ataques internos

Explicación

Código malicioso	Software diseñado para explotar vulnerabilidades del sistema y extraer información o tomar control de los datos. Se presenta de las siguientes maneras: ○ **Virus:** programa que puede hacer copias de sí mismo y extenderse a otros. ○ **Gusanos:** *malware* diseñado para extenderse de una computadora a otra. ○ **Caballos de Troya**: programa que parece ser benigno pero luego hace algo inesperado. ○ **Puertas traseras**: característica de virus y gusanos que permiten a un atacante acceder remotamente a una computadora comprometida. ○ **Redes de *bots***: código que se puede instalar en una computadora y responder a comandos maliciosos de externos.
Programas potencialmente no deseados	Software que se instala a sí mismo en una computadora, por lo general, sin el consentimiento informado del usuario. Se presenta de las siguientes maneras**:** ○ ***Adware*:** programa que hace aparecer publicidad emergente. ○ **Parásito del navegador**: programa que puede monitorear y modificar la configuración del navegador. ○ ***Spyware* (programa espía)**: software que se usa para obtener información como las teclas pulsadas, cuentas o contraseñas.

Explicación

***Phishing* y robo de identidad**	Cualquier intento engañoso habilitado en línea por parte de alguien que quiere obtener información confidencial a cambio de un beneficio económico. Generalmente explota la falibilidad e ingenuidad humanas para distribuir malware. Se presenta de las siguientes maneras**:** ○ Estafas por correo electrónico. ○ Intento de suplantar a un banco para recibir datos de las cuentas de los clientes.
Hacking	Los hackers son individuos que intentan acceder a un sistema sin autorización. Se presenta de las siguientes maneras**:** ○ ***Crackers*:** son hackers con fines delictivos. ○ **Hackers de sombrero blanco (*White hat*):** buscan ayudar a la empresa a encontrar fallas. ○ **Hackers de sombrero negro (*Black hat*):** buscan ocasionar daños. ○ **Hackers de sombrero gris (*Grey hat*):** actúan con buenas intenciones al creer estar persiguiendo un bien mayor al irrumpir en los sistemas. Son un híbrido entre los hackers de sombrero blanco y de sombrero negro.

Explicación

Vandalismo cibernético	Su finalidad es interrumpir, desfigurar y/o destruir los sitios web.
Filtración de datos	Se refiere a la pérdida de control sobre la información corporativa a manos de intrusos.
Fraude con tarjetas de crédito/robo	Los hackers atacan a los servidores mercantiles y, con ello, pueden utilizar los datos robados para establecer un crédito con una identidad falsa.
Spoofing (pharming)	Se refiere a presentarse con direcciones falsas o hacerse pasar por otra persona.
Ataque de negación de servicio (DoS, por sus siglas en inglés, *Denial of Service*)	Los hackers inundan un sitio con tráfico inútil para abrumar la red, se puede hacer desde una (DoS) o varias computadoras coordinadamente (DDoS).
Husmeador *(sniffing)*	Programa de espionaje que monitorea la información que viaja a través de una red.
Ataques internos	Ataques realizados por personal interno de la empresa.

Explicación

Soluciones y políticas de seguridad

Entre las **soluciones tecnológicas** para los ataques o amenazas en el entorno cibernético, se encuentran las siguientes:

- La protección de las comunicaciones de Internet mediante cifrado (encriptación).
- Proteger los canales de comunicación de SSL (*Secure Sockets Layer*) y VPN (*Virtual Private Network*).
- Proteger las redes con Firewalls.
- La protección de servidores y clientes.

Desarrollo de un plan de seguridad en el comercio electrónico

1. La valoración del riesgo es el análisis de los riesgos y puntos de vulnerabilidad.
2. La política de seguridad es el conjunto de estatutos que identifican y priorizan los riesgos y determinan los mecanismos necesarios para alcanzar estos objetivos.
3. El plan de implementación incluye los pasos necesarios para lograr los objetivos del plan establecido.
4. Una organización de seguridad educa y capacita a los usuarios, brindando el mantenimiento necesario a las herramientas y políticas definidas.
5. Una auditoría de seguridad consiste en revisar rutinariamente los registros para determinar si el plan ha funcionado.

Explicación

Sistemas de pago en el comercio electrónico

Los **participantes en un sistema de pago** son el consumidor, comerciante, intermediarios financieros y los reguladores del gobierno. Cada uno de los actores tiene objetivos claros:

- El **consumidor** busca bajo riesgo, bajo costo, refutabilidad, comodidad, y fiabilidad.
- El **comerciante** busca: bajo riesgo, bajo costo, irrefutabilidad, seguridad y fiabilidad.
- Los **intermediarios financieros** quieren que el sistema de pago sea seguro y de bajo riesgo, así como de maximización de beneficios.
- A **los reguladores del gobierno** les interesa la seguridad, confianza y protección para los participantes.

A continuación se muestra un ejemplo de una transacción en línea realizada con tarjeta de crédito:

1. La compra.
2. La entrega del pedido al comerciante mediante una conexión segura SSL.
3. La transferencia de la orden de la cámara de compensación a través de una línea segura.
4. La verificación con el banco emisor del consumidor de la disponibilidad de un saldo suficiente para realizar la compra.
5. Abono del banco emisor a la cuenta de los comerciantes.
6. El envío al consumidor de un estado de cuenta mensual que incluye el cargo.

Actividad

Instrucciones

- Investiga y documenta cuál es la diferencia entre una dirección HTTP y una HTTPS.

Cierre

En este tema se resumen las amenazas de seguridad y las soluciones que los administradores de sitios de Internet tienen que conocer, aunado a la comprensión de los diferentes sistemas de pago disponibles en la web.
La seguridad cibernética es un fenómeno complejo y multifacético que involucra un conjunto diverso de riesgos y un enfoque equilibrado.

Para lograrlo, es fundamental contar con tres elementos:
1. Implementación de tecnología orientada a proteger y salvaguardar la seguridad de los usuarios, equipos e información.
2. Políticas y procedimientos de la organización.
3. Leyes y normas de la industria.


Universidad
Tecmilenio®

Universidad Tecmilenio

Gestión avanzada de Tecnologías de la Información

Aspectos éticos y sociales del comercio electrónico

Introducción

El uso de Internet ha traído inmensas ventajas a la sociedad, empezando por el intercambio de bienes y servicios y terminando con las posibilidades de llevar
educación y cultura hasta los lugares más alejados de la civilización. Esto no significa que el Internet no pueda ser utilizado para fines nocivos o la comisión de delitos.

Las libertades de expresión e información existentes en Internet requieren una protección jurídica:

- La dignidad humana frente al peligro que representan las páginas web que incitan a la discriminación racial, cultural o social.
- La niñez de cara a la difusión de la pornografía o de formas extremas de violencia.
- La propiedad intelectual frente a la distribución no autorizada de trabajos científicos, musicales o programas de cómputo.
- La seguridad nacional, que se ve amenazada cuando se difunden instrucciones para el armado de bombas o producción de drogas.

Como podemos ver, en el desarrollo de la red de redes se han perfilado varios
campos de posible conflicto debido a la ausencia de reglas suficientemente claras (Trejo, 2006).

Trejo, E. Arámbula, A., Álvarez, M. (2006). *Regulación Jurídica de Internet.* Recuperado de https://bit.ly/3L4PRgs

Explicación

El Internet y la ética

Al igual que otras tecnologías, el Internet puede habilitar nuevos tipos de crímenes, afectar el medio ambiente y amenazar los valores de la sociedad. A su vez, la rapidez con la que el Internet alcanzó su popularidad (en comparación con otras tecnologías), hizo muy difícil que se desarrollaran leyes y costumbres adaptadas a la nueva realidad. Por ello, los costos y beneficios se deben analizar con cuidado, especialmente cuando no existen guías legales claras.
Existen cuatro elementos que comparten todas las corrientes éticas occidentales:

Responsabilidad	La **responsabilidad** trata de que como agentes morales libres, los individuos, las organizaciones y la sociedad son responsables por las acciones que realizan.
Impuntualidad	La **impuntualidad** se refiere a que los individuos, empresas y sociedad deben responder ante otros por las consecuencias de sus actos.
Obligatoriedad	La **obligatoriedad** es una ley que permite a los individuos obtener una reparación por los daños que hayan recibido por parte de otros actores, sistemas u organizaciones.
Derecho al proceso	Finalmente, el **derecho al proceso** que hace referencia al proceso por el que las leyes son conocidas y comprendidas. En este proceso existe la posibilidad de recurrir a autoridades superiores para hacer que se apliquen como corresponda.

Explicación

Derecho de privacidad y de información

Los efectos del Internet se pueden analizar desde el punto de vista individual, social y político. Existen **cuatro dimensiones morales** que se deben considerar:

1	2	3	4
Derecho a la información	**Derecho de propiedad**	**Gobernabilidad**	**Seguridad y bienestar públicos**
○ ¿Qué derecho sobre su información personal tienen los individuos en un mercado público, o en sus hogares, cuando las tecnologías hacen la información ubicua y eficiente? ○ ¿Qué derecho tienen las personas de acceder a información de empresas?	○ ¿Cómo se pueden proteger los derechos de propiedad intelectual en un mundo donde el costo de hacer y distribuir copias exactas de una obra es casi cero?	○ ¿Debe Internet ajustarse a las leyes de algún país? ○ ¿Quién tiene jurisdicción, el gobierno federal, el estatal o el local?	○ ¿Se debe asegurar el acceso equitativo a la red? ○ ¿Debe el gobierno garantizar el acceso a Internet desde las escuelas?

Explicación

Directivas de privacidad

Las empresas estadounidenses pueden reunir y redistribuir información de una transacción sin el **consentimiento informado** del individuo, lo que sería ilegal en Europa. El **consentimiento informado** es la aceptación que se da con conocimiento de todos los hechos materiales necesarios para tomar una decisión racional.
Existen dos tipos de consentimiento informado:

Entrada opcional (*Opt-in*)

Requiere una acción afirmativa por parte del consumidor para permitir que se utilice la información

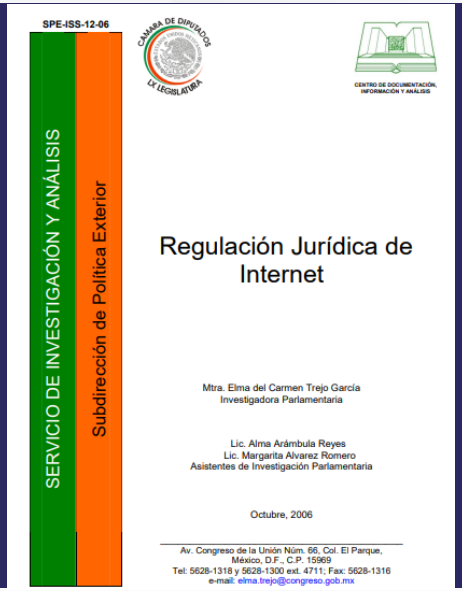
Salida opcional (*Opt-out*)

Se recaba de antemano la información a menos que el consumidor explícitamente lo prohíba.

Actividad

Instrucciones

- Haz un resumen del documento de Regulación Jurídica de Internet elaborado en la Cámara de diputados: http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-12-06.pdf



Cierre

Es importante considerar que, aunque el Internet abra las puertas a manejos poco éticos de la información e invasión de la privacidad, las empresas deben implementar un lineamiento empresarial con base en la honestidad y buenas prácticas. Esta implementación tiene su precio y, aunque en ocasiones a corto plazo no se visualice el resultado esperado, las consecuencias de “hacer las cosas mal” pueden ser enormes, como posibles litigios que son potencialmente negativos para el negocio.

Por otro lado, el concepto de privacidad suele tomar gran relevancia debido a su vulnerabilidad en el mundo cibernético. Al existir diferentes herramientas y plataformas para facilitar la comunicación entre usuarios a nivel global, cada vez es más complicado poder controlar y garantizar la privacidad de información de estos. Sin embargo, poco a poco se han venido estableciendo leyes y reglamentos con la finalidad de poder regular este aspecto.


Universidad
Tecmilenio®

Universidad Tecmilenio

Gestión avanzada de Tecnologías de la Información

Asuntos legales

Introducción

Este tema se refiere a la protección de los derechos de autor para proteger los derechos intelectuales de la publicación de la obra (*copyright*), debido a que por Internet se puede consultar y hacer uso de información generada en cualquier parte del mundo, y existe la posibilidad de que alguien se apropie de la autoría de obras que elaboraron otras personas, siendo esto un delito.

Kevin Chaires (2021), en su trabajo Derechos de autor en la era digital, todo lo que debes saber, en entrevista a Diana Sánchez, abogada litigante y socia fundadora en **ODH-Asesores**, explica lo siguiente:

¿Qué se puede registrar?

"Lo que protegen los Derechos de Autor no son las ideas que uno puede tener como artista, ***sino la expresión de estas.*** *Antes era pintura en lienzos, pero ahora contamos con cuestiones digitales"*, explica la abogada.

En México, las obras son salvaguardadas por el **Instituto Nacional de Derechos de Autor.** Si alguien explota nuestra obra sin nuestro consentimiento, este organismo es el que nos protege.

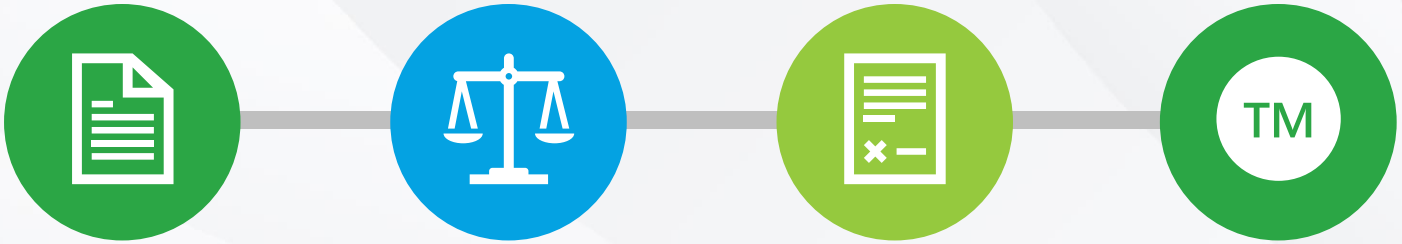
"Esto cuenta con una caducidad de 100 años después de la muerte del autor. Tras pasar este periodo, entran en ***dominio público*** *y ya no se debe pedir permiso para utilizarlos"*.

Chaires, K. (2021). *Derechos de autor en la era digital, todo lo que debes saber.* Recuperado de https://bit.ly/37Z8Tqt

Explicación

Derechos de propiedad intelectual

Después de la privacidad, el aspecto ético, social y político, lo más controvertido en relación con el comercio electrónico son los derechos de la propiedad intelectual, lo cual engloba todos los productos tangibles e intangibles existentes.
Existen cuatro **formas de protección de la propiedad intelectual**:



Patentes | **Derechos de autor** | **Secretos industriales** | **Marcas**

Las **patentes** otorgan al dueño un monopolio exclusivo de las ideas atrás de la invención por 20 años (10 años para modelos de utilidad). Se pueden patentar mecanismos, productos hechos por el hombre, fórmulas y procesos o métodos.
Los **derechos de autor** protegen formas originales de expresión (pero no ideas) por un periodo de tiempo, generalmente, durante la vida del autor y 75 años adicionales. Se pueden registrar obras de arte, libros, películas, fotografías, canciones y otras obras que representen formas de expresión. La ley otorga al titular de los derechos de autor la opción de decidir qué hacer con su obra, autorizar a otros a difundirla o no y decidir cuánto cobrar y qué uso se le puede dar a su obra.
Un **secreto industrial** protege una obra intelectual utilizada para fines de negocio, siempre y cuando no sea del dominio público. Se obtiene manteniendo la información confidencial.
Se usa una **marca**, nombre o producto registrado legalmente para distinguir los bienes de una persona. Una marca asegura que el consumidor obtiene lo que paga o espera recibir y protege al propietario contra la piratería y la apropiación indebida.

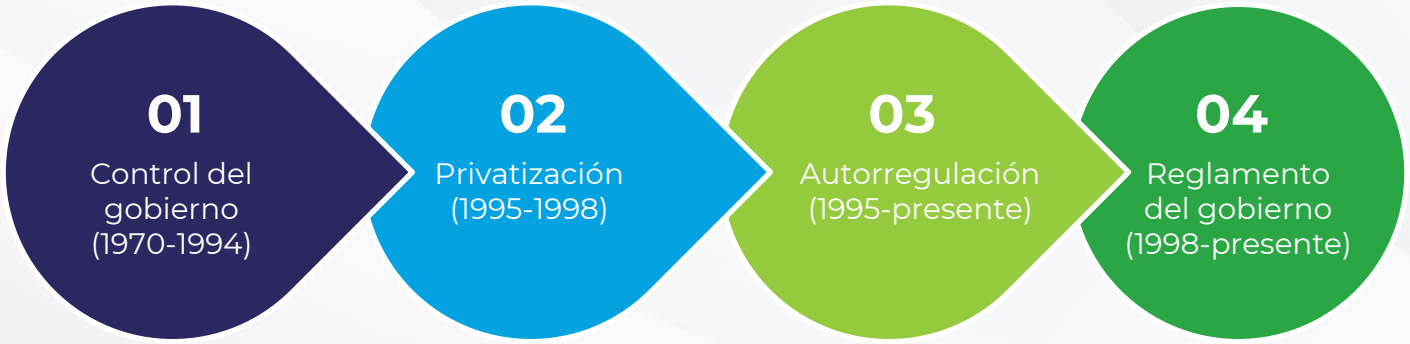
Explicación

Gobernanza

La **gobernanza** tiene que ver con el control social de la red:

- ¿Quién va a controlar al Internet y el comercio electrónico?
- ¿Qué elementos se controlarán y cómo?

Al analizar la evolución de la gobernanza en Internet se aprecian cuatro periodos:



Explicación

Control del gobierno (1970-1994)	La DARPA (*Defense Advanced Research Projects Agency*) y la NSF (*National Science Foundation*) controlan el Internet como un programa totalmente patrocinado por el gobierno.
Privatización (1995-1998)	*Network Solutions, Inc.* recibe el monopolio de asignar y dar seguimiento a los dominios de alto nivel de Internet. La columna vertebral se vende a compañías privadas de telecomunicación. Los aspectos de política permanecen sin decidir.
Autorregulación (1995-presente)	El Gobierno de los Estados Unidos estimula la creación del ICANN (*Internet Corporation for Assigned Names and Numbers*) para manejar los conflictos emergentes y establecer políticas.
Reglamento del gobierno (1998-presente)	Organismos mundiales comienzan a implementar controles directos sobre el Internet y el comercio electrónico.

Explicación

Seguridad y bienestar público

Los gobiernos de todo el mundo afirman que buscan el bienestar del público y por eso producen leyes para controlar todo, desde el uso de las calles hasta qué podemos ver en televisión. Los medios electrónicos han sido históricamente regulados y el Internet no es una excepción.

Actividad

Instrucciones

- Documenta cuáles son los requisitos y pasos a seguir en México para el registro de una patente.

Cierre

Este tema define los derechos de propiedad intelectual y describe las formas en que se pueden proteger los siguientes:

- Derechos de autor
- Patentes
- Marcas
- Secretos industriales

Con respecto a cuestiones de **gobernanza**, durante los primeros años del comercio electrónico se acostumbraba a pensar en el Internet como una tecnología demasiado poderosa para cualquier control del gobierno. Ahora sabemos que el Internet, o al menos los jugadores clave como ISP, sitios de comercio electrónico y de telecomunicaciones, se pueden controlar al igual que en otras formas de medios de comunicación.