Ingeniería en Desarrollo de Software
Semestre 8

Programa de la asignatura:
Programación web II

Unidad 2. Mi sitio web dinámico y seguro

Ciudad de México, mayo del 2025

Clave:
15144843

Universidad Abierta y a Distancia de México

Índice

Unidad 2. Mi sitio dinámico y seguro 3
Presentación de la Unidad 3
Logros 3
Competencia específica 4
1. Seguridad y posicionamiento de un sitio web 4
1.1. Autenticación 5
1.2. Manejo de sesiones 7
1.3. Validación de datos 8
1.4. Visibilidad de un sitio web 10
2. Derechos de autor 12
2.1. Los derechos de autor y las tecnologías web 13
2.2. Derechos de autor y protección en internet 17
3. Conexión segura a bases de datos 18
Para saber más 28
Cierre 29
Fuentes de consulta 30
Bibliografía complementaria 32
Fuentes de imagen 32

Unidad 2. Mi sitio dinámico y seguro

Presentación de la Unidad

En esta segunda unidad aprenderás acerca de la seguridad de un sitio web, aprenderás como hacer sitios seguros y confiables para los usuarios. Asimismo, aprenderás cómo hacer tu sitio web más visible para los usuarios; es decir, a posicionar a tu página web en las primeras listas que se obtengan al realizar búsquedas en la web. Para ello, aprenderás acerca de las herramientas que puedes usar y aplicar a tu página web para que pueda llegar más fácilmente a más usuarios. Comprenderás los derechos de autor para no infringir la ley al usar en tu página web material que esté protegido por estos derechos, como textos, imágenes, sonidos, música o videos.
Y finalmente aprenderás cómo usar bases de datos en forma segura en tu página web.

Consideraciones de seguridad generales para una página web
Cuando se planea el diseño de una aplicación web, es de vital importancia considerar las siguientes normas generales de seguridad básicas:

- Autenticación de usuarios.
- Validación en la entrada y salida de información.
- Utilización de mecanismos de seguridad simples.
- Utilización y reutilización de componentes de confianza.
- Defensa en profundidad.
- No haber lugar a la confianza.
- Definición y verificación de privilegios.
- No presentar más información que la pertinente a cada usuario.

Logros

Al término de esta unidad lograrás:

- Conocer e identificar los diferentes elementos de seguridad que existen en la actualidad y que puedes integrar en una página web.
- Dominar las herramientas que te permitan hacer más visible tu sitio web; es decir, posicionar tu página web entre las primeras de las listas al realizar búsquedas en la web.
- Reconocer los objetos que pudieran estar protegidos por los derechos de autor para usarlos en tu página web y así no caer en el robo o plagio de propiedad protegida por los derechos de autor.

Competencia específica

- Aplicar elementos de seguridad a nuestra página web y conocer toda la información sobre losderechos de autor para no usar elementos que estén protegidos por estos derechos.

1. Seguridad y posicionamiento de un sitio web

“La seguridad en el web es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios del web y las organizaciones que los rodean. La seguridad es una protección contra el comportamiento inesperado” (Garfinkel, 1999).

Internet es hoy en día una de las herramientas de más uso a nivel mundial, debido a lo cual cada día hay más personas que se integran al uso de éste para diversos objetivos, lo que a su vez implica que cada día también se deba pensar en mejores medidas de seguridad, tanto para quien proporciona los servicios como para quienes hacen uso de éstos, ya que existe un sinnúmero de amenazas circulando diariamente por internet, algunas de ellas creadas con propósitos específicos y algunas otras para generar daño al azar. Existen también muchas personas que se dedican a estudiar las diferentes vulnerabilidades que pueden presentar los sitios y aplicaciones web, y tales personas hacen uso de ellas para generar algún tipo de daño o sacar provecho de las mismas.

Por ello, cuando se habla de seguridad en la web, se está refiriendo a medidas que se aplican a varios componentes de ésta, por ejemplo, servidores, bases de datos, lenguajes, usuarios, etc.

Está comprobado que gran parte de las vulnerabilidades que existen en la web hoy en día son debido a las aplicaciones; esto provocado por las malas prácticas de desarrollo e implementación bajo las que se crean y se ponen en producción a dichas aplicaciones, es decir, que no se cumplen o no se aplican de forma adecuada las normas básicas o estándares de seguridad sugeridos según los lenguajes utilizados para el desarrollo de las mismas.
A continuación, se exponen los principales problemas de seguridad de un sitio web:

Vulnerabilidades
“El término *vulnerabilidad*, se emplea para referirse a todos los puntos débiles o frágiles que se considera que tiene un programa determinado, y que pueden hacer que aquel sea atacado por virus de diversa tipología.

“De la misma forma, cuando un archivo o un software se dice que tiene problemas de vulnerabilidad, se está haciendo referencia a que tiene vacíos de seguridad que pueden permitir la entrada de intrusos y piratas que puedan poner en peligro su confidencialidad o integridad.” (MSDN, 2014).

Las principales vulnerabilidades que pueden presentarse en una aplicación web son:

- Autenticación
- Manejo de sesiones
- Validación de datos

1.1. Autenticación

La autenticación en una aplicación web que consiste en la comprobación o identificación de un usuario válido y con permiso activo para el ingreso a la misma.

Existen dos formas en las que se puede realizar una autenticación:

1. La autenticación delegada en el servidor y cliente.
"Mediante la autenticación delegada, un servidor delega la autenticación de un usuario final en otro servidor. El equipo cliente envía una solicitud al primer servidor, el cual envía a su vez una o más solicitudes a un segundo servidor por parte del usuario final. Para realizar esta operación correctamente, el primer servidor debe delegar la autenticación de los usuarios finales en un segundo servidor, lo que requiere una de estas dos relaciones de confianza" (MSDN, 2014):

- El cliente confía al primer servidor su contraseña, por ejemplo, para usar la autenticación básica o un almacén de credenciales del servidor, como el mecanismo de inicio de sesión único conectable de Microsoft Office SharePoint Server 2007 o los Servicios de federación de Active Directory (ADFS).
- El segundo servidor confía en el primer servidor para pasar credenciales válidas con fines válidos como, por ejemplo, para establecer una relación de confianza de delegación limitada de Kerberos entre los servidores.

Pueden ser:

- Basados en estándares de internet, dentro de los cuales encontramos a:
  - Autenticación básica HTTP
  - Autenticación digest HTTP
  - Autenticación del Cliente HTTPS
- Basados en la especificación de servlets
  - Autenticación basada en formularios

Implementación
"Para filtrar los datos proporcionados por el usuario del lado del servidor, se recomienda el empleo de listas blancas, las cuales pueden generarse a partir del empleo de expresiones regulares.

“Ejemplo. Para guardar la edad de un usuario, se tiene la siguiente expresión en la que se asigna directamente el valor obtenido de un formulario a una variable.

```
$edad=$_POST['edad'];
```

Si el dato no se valida correctamente, pueden ingresarse cadenas de código malicioso para obtener información de la aplicación o de sus usuarios. A continuación se presenta una alternativa para su validación” (UNAM-CERT, 2014):

```
$edad_recibe = $_POST['edad'];
$regexp_edad = '^[0-9]{1,2}$';
$edad_valida = preg_match($regexp_edad,$edad_recibe);
if($edad_valida)
      $edad = $edad_recibe;
else
      $error = "se debe ingresar una edad entre 0 y 99";
```

2. La autenticación controlada por programa es aquella en la que el desarrollador tiene la tarea de realizar la autenticación dentro de la aplicación misma, ya sea mediante el uso de nombres de usuario y contraseñas almacenadas en una fuente, como una base de datos, o utilizando algún método alternativo de almacenamiento de éstas.

Ejemplo de almacenamiento de información (Bases de datos)

“La información es el elemento más importante que se maneja por las aplicaciones web, por lo que se debe proteger.

“Es muy importante tomar las medidas necesarias para disminuir el acceso de personas no deseadas a la información manejada por la aplicación.

“Implementación

“El servicio de bases de datos debe configurarse de forma segura haciendo **hardening** a la configuración, evitar usuarios, contraseñas y configuraciones por defecto” (UNAM-CERT, 2014):

Código:

Al instalar un manejador de bases de datos, crear un usuario que sea el dueño de la base de datos y sólo pueda tener acceso a ella:

```
postgres=# create user aaguilar encoding password ‘secreto1’;
postgres=# create database pruebas1 owner aaguilar;
```

Riesgos de implementación inadecuada

Extracción o modificación de información de la base de datos (del servicio y del contenido).

La **autenticación** es una forma de seguridad para validar que los usuarios correctos puedan acceder a su información por medio del uso de claves de acceso, usuarios y passwords, así como validaciones de datos personales.

Otra de las principales vulnerabilidades que puede presentar una aplicación es el manejo de sesiones, tema que se explica a continuación.

1.2. Manejo de sesiones

El manejo de sesiones en aplicaciones web se realiza con base en herramientas que proporcionan los lenguajes de programación y permiten asociar información de un usuario en específico durante el tiempo que permanezca activo en la aplicación.

Por ejemplo, el lenguaje PHP tiene algunos comandos y funciones que permiten implementar el proceso de autenticación y seguimiento de las diferentes actividades que realice el usuario en cuestión, dentro de la aplicación, ya que en éstas, por lo general, existen partes que son privadas, y de acuerdo al tipo de usuario es el nivel de acceso que se le puede otorgar (Unijimpe, 2011).

Este proceso, al estar correctamente implementado en una aplicación, facilita las tareas de control y supervisión de accesos, pero si no lo está, puede presentar o volverse en sí mismo una vulnerabilidad que contraste con la seguridad de ésta.

Todas las variables de sesión son accesibles mediante *arrays* en la variable global `$_SESSION`. Adicionalmente, ofrece una serie de funciones que permiten manejar detalladamente las sesiones de manera sencilla (Unijimpe, 2011):

- `session_start` inicializa una sesión y crea el identificador de sesión.
- `session_id` devuelve el identificador de la sesión actual.
- `session_regenerate_id` genera un nuevo identificador para la sesión actual.
- `session_unset` limpia todas las variables de sesión registradas.
- `session_destroy` elimina todas las variables de sesión registradas.

Crear variables de sesión

Si deseamos crear variables de sesión para que se puedan utilizar a través de diferentes páginas, inicializamos el manejo de sesiones con la función `session_start` y luego

guardamos el dato deseado como variable de sesión, utilizando la variable global `$_SESSION`. (Unijimpe, 2011):

```
// home.php
session_start();
$_SESSION["country"] = "Peru";
```

Incluso se podría mejorar el código si se verifica la existencia de la variable de sesión; si no existe, entonces le asignamos un valor.

```
// home.php
session_start();
if (!isset($_SESSION["country"])) {
        $_SESSION["country"] = "Peru";
}
```

1.3. Validación de datos

La validación de datos es el proceso mediante el cual los datos son filtrados y aceptados o rechazados de acuerdo a procedimientos definidos. Los procedimientos son definidos por las necesidades de las aplicaciones, que generalmente atienden a las necesidades de los usuarios de las mismas (Flores, 2014).

Existen elementos dentro de los lenguajes de programación utilizados que permiten realizar validaciones de forma automática sin la necesidad de agregar código para ello, pero también se puede crear un proceso de validación de la información mediante la codificación de los mismos. Estos elementos son los controles de validación que cada lenguaje tiene.

Por ejemplo, en ASPNET se tienen las principales propiedades que se aplican a todos los controles de validación, las cuales se muestran en la siguiente tabla (UDB, 2014):

Propiedad	Descripción
ControlToValidate	Id. de programación del control de salida que evaluará el control de validación. Si no es un Id. Legítimo, se iniciará una excepción.

Display	Modo en que se muestra el control de validación especificado. Esta propiedad puede ser uno de los siguientes valores: Ninguno — El control de validación jamás se muestra en línea. Utilice esta opción cuando desee mostrar el mensaje de error sólo en un control **ValidationSummary** Estático — El control de validación muestra un mensaje de error si se produce un error en la validación. Se asigna un espacio en la página web para el mensaje de error incluso si el control de entrada supera la validación. No cambia el diseño de la página cuando el control de validación muestra su mensaje de error. Como el diseño de página es estático, si hay varios controles de validación para el mismo control de entrada, éstos deberán ocupar distintas ubicaciones en la página. Dinámico — El control de validación muestra un mensaje de error si se produce un error en la validación. El espacio para el mensaje de error se asigna dinámicamente en la página cuando se produce un error en la validación. De este modo, varios controles de validación pueden compartir la misma ubicación física en la página.
EnableClientScript	Indica si está habilitada la validación en el cliente. Para deshabilitar la validación en el cliente en los exploradores que admitan esta función, establezca la propiedad **EnableClientScript** en *false*.
Enabled	Indica si está habilitado el control de validación. Para impedir que el control de validación valide un control de entrada, establezca esta propiedad en *false*.

Propiedades de controles de validación (UDB, 2014)

El proceso de validación de datos es muy importante, ya que con éste se verifica la integridad de la información y se monitorea de forma permanente que no exista filtrado o inyección de información ajena a la que el usuario o usuarios están generando.

Para mantener una adecuada validación de datos deben considerarse las siguientes acciones:

- Verificar la exactitud de los datos críticos, independientemente de la fuente de los mismos.
- Realizar validaciones de forma rutinaria para identificar posibles errores.
- Utilizar procedimientos estandarizados para la definición de datos sin procesar, seguridad para la entrada y revisión.
- Llevar un registro de las fallas o eventos inusuales que ocurran.
- Debe llevarse un registro de quien realiza cambios a los datos originales.

1.4. Visibilidad de un sitio web

La **visibilidad web** es el objetivo que debe alcanzar cualquier organización que quiera tener éxito en internet. Consiste en destacar los contenidos, productos y servicios ofertados en internet, de manera que los usuarios los reconozcan, adquieran y accedan ellos. (Biblioseo, 2012)

García (2010) define la **visibilidad web** como un conjunto de actividades y elementos que posibilitan y facilitan la localización de un sitio web en internet. Es decir, que el usuario, sin hacer mayor esfuerzo en el diseño de estrategias de búsqueda, pueda localizar la información de una manera sencilla y ágil.

Por su parte, Aced y Arqués (2010) definen la **visibilidad web** como una actividad necesaria para tener éxito en internet, donde los usuarios reconozcan, compren y consuman los contenidos, productos y servicios ofertados en un sitio web. De igual manera, resaltan que hablar de visibilidad es ocuparse de la reputación de los contenidos, productos y servicios ofrecidos, puesto que en la sociedad en red es imposible tener control sobre la información que se publica.

En internet se encuentran el 95% de tus clientes potenciales, leyendo blogs, revisando su correo, navegando por Facebook o buscando en Google, y no deberías desechar la oportunidad que tienes de darte a conocer en alguno de estos medios y conseguir así nuevos clientes o usuarios (Ventura, 2011).

A continuación, exponemos 10 formas de dar a conocer tu página web en internet para ganar visibilidad, según Ventura (2011):

1. Crear un blog
Es importante escribir artículos de calidad que estén relacionados con el negocio que promocionamos con la página web para atraer al público deseado y que dicho público reciba información que le sea de utilidad, escrita por un profesional de la materia, para que el cliente decida por los productos que promociona dicho profesional.

2. Participa en las redes sociales
Las redes sociales hoy en día son un medio de publicidad muy importante porque siempre encuentras a mucha gente participando en ellas. Hay algunas redes sociales especializadas en donde podemos encontrar clientes potenciales; entre estas redes sociales tenemos Facebook, Twitter y Linkedin.

3. Consigue enlaces en sitios web de relevancia o de tu propio nicho de mercado

Es importante considerar el tener muchos enlaces desde diferentes sitios que vayan a tu página web; esto hará que tu sitio gane relevancia, lo cual, a su vez, es premiado por Google, Yahoo! o Bing, mostrándote más arriba en las búsquedas relacionadas con esos temas.

4. Crea un video y súbelo a un sitio de amplio alcance
Esto hará que se posicionen bien y rápidamente entre los resultados de búsqueda de Google.

5. Escribe como invitado en otro blog
Si no tienes tiempo de mantener tu propio blog, o no tienes suficientes artículos que escribir para lograr una publicación constante, puedes considerar el escribir artículos para otros blogs, ya que igualmente te darán cierta reputación y nuevas visitas, además de que no te obligará a escribir tan estrictamente como lo harías al tener tu propio blog o un blog de empresa.

Si eres experto en tu sector, también puedes realizar entrevistas para blogs y revistas online, que en la mayoría de los casos estarán encantados de publicar, ya que para ellos será material “gratis”. Eso sí, no te olvides de pedir que incluyan un enlace, así como una referencia a tu negocio o a ti mismo, para que el esfuerzo merezca totalmente la pena.

6. Optimizar tu página web para los buscadores
Si optimizas de forma correcta tu sitio web, y tienes contenido fresco y de calidad, poco a poco y de forma natural irás escalando posiciones en los resultados de búsqueda y los usuarios podrán encontrarte realizando las búsquedas por las que quieres aparecer.

7. Participación con comentarios de calidad en blogs y foros
Participar en otros blogs, foros, etc., no sólo sirve para conseguir colocar otro enlace nuevo; sirve, sobre todo, para darte a conocer, crear una imagen profesional y de experto en el tema, lo cual te ayudará a captar nuevos clientes. Comenta las noticias o artículos más importantes, aportando una nueva visión o algún consejo, y habla de tu proyecto para que sepan quién eres. En estos blogs o foros se encuentra tu público objetivo, así que puedes aprovechar y llevarte unos cuantos hacia tu negocio.

8. Crear o utilizar un programa de afiliados, partners, comisiones por ventas
Existen muchas formas de conseguir que otros vendan tus productos u ofrezcan tus servicios a cambio de una pequeña comisión. Normalmente, esta comisión vendrá ligada a una venta realizada o a cualquier conversión que nosotros estipularemos, por lo que no tendremos que adelantar ningún pago.

Los programas de afiliación son los más utilizados. En ellos, tú, como anunciante, ofreces tus condiciones y una comisión por venta. Mediante un banner o un enlace, otros **bloggers** y **webmasters** ofrecerán tus productos e intentarán venderlos en sus blogs o sitios web. Este

programa registrará las ventas o conversiones realizadas y pagará/cobrará automáticamente lo que corresponda.
Sin embargo, no hace falta participar en un programa de afiliación. Puedes acordar personalmente las comisiones de venta con quien desees, y mediante Google Analytics u otro programa que rastree las ventas, saber cuántas conversiones han llegado por cada vía, y poder pagar así la comisión que corresponda.

9. Realizar una campaña publicitaria en Google Adwords
Anunciarse en internet es el mejor método de captar al público del mismo internet, y Google Adwords es una excelente opción. Pero tiene un costo que vale la pena pagar si deseas posicionar tu página web en la primera página de búsquedas de Google.
10. Déjalo en manos de profesionales
En ocasiones, el emprendedor no dispone del tiempo ni de los conocimientos necesarios para llevar a cabo los pasos necesarios. En ese caso, y viendo la importancia de la visibilidad en internet, lo mejor es dejarlo en manos de profesionales, que sabrán conseguir los resultados deseados de forma óptima y en un tiempo menor de lo que podrías lograr por tu cuenta.

Consulta el tema sobre posicionamiento de un sitio web en el recurso *U1. Posicionamiento* en la carpeta *Materiales para el desarrollo de la Unidad 2.*

2. Derechos de autor

En la actualidad las organizaciones realizan sus sistemas de tipo web debido a que este tipo de sistemas facilita al usuario el manejo de la información. Asimismo, se debe tomar en cuenta que con el uso de las tecnologías en internet pueden ocurrir pérdidas de los datos, por lo que se debe tener un control la integridad de los mismos.

En relación a lo anterior, como ingeniero en Desarrollo de software necesitas saber cuál es el impacto y lugar que tienen la seguridad de datos en la web. Para ello, en el primer tema de esta unidad estudiarás los conceptos básicos relacionados con la seguridad, posicionamiento en la web y los derechos de autor, y finalmente con la conexión segura a base de datos.

En la actualidad muchas actividades que realizan las organizaciones, como, por ejemplo, publicidad, educación, difusión de información, etcétera, son publicadas mediante el uso de internet y la publicación de sitios que son diseñados por expertos en el área de informática; sin embargo, existe un problema prioritario, y es el de la piratería o el plagio de información.

Otro aspecto en la era digital es la aplicación de la ley del derecho de autor para proteger a los autores de desarrollo tecnológico. En este tema se pretende analizar qué es el derecho y quiénes interfieren en el proceso de publicación en la web.

“Cuando aparecieron las nuevas tecnologías de la información y la comunicación, emergió una nueva y asombrosa forma de publicar, con un proceso menos complicado, relativamente costoso y sin papel. En los inicios de los noventa, cuando internet entró en su apogeo, aún no existía la preocupación por el derecho de autor en la red y se multiplicó, entonces, el entusiasmo por publicar periódicos y revistas, principalmente. Además, se preveía el comportamiento de la red como un campo propicio para los investigadores y los escritores, quienes no sentían recelo alguno por dar a conocer su información en una plataforma abierta y de acceso universal” (López y Estrada, 2007).

Asimismo, se requiere identificar la propiedad intelectual del derecho de autor, el derecho industrial y el derecho de obtentores.
Para entender qué es el derecho de autor, en primer lugar, se explicará el significado de derecho:“El derecho en sentido objetivo, es el conjunto de normas jurídicas que gobiernan la conducta externa de los hombres en sociedad y que se impone a los mismos en virtud de la coercitividad que el Estado ejerce al aplicar sanciones a quien la viole.” (Nolasco, 2005)

Ya explicado el concepto, ahora se explicará que el derecho de autor, según la ley federal de autor, es: “El reconocimiento que hace el estado en favor de todo creador de obras literarias y artísticas previstas en el artículo 13 de esta ley, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial.” (Instituto Nacional del Derecho de Autor, México, 2014)

En otras palabras, el derecho de autor es el reconocimiento que hace el estado a favor del creador de la obra.

2.1. Los derechos de autor y las tecnologías web

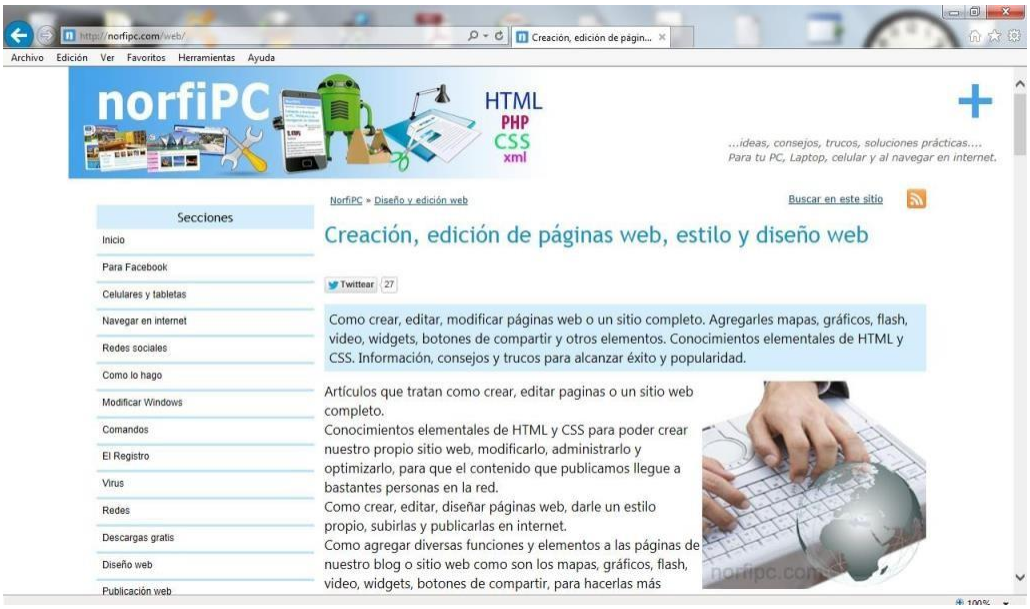
En la actualidad se ha visto la necesidad de establecer lineamientos para evitar el plagio de la información, por lo que debemos establecer quienes participan en el proceso de derechos de autor, especialmente en las tecnologías web.

Protagonistas en los derechos de autor para la Web (DNDA, 2014):

Autor. Es la persona responsable de la creación del sitio web, artículo, animación. También se establece que no se requiere registrar la creación del mismo, pero sí cumplir con dos propiedades fundamentales del registro:

- Recurso web
- Contenido del derecho de autor

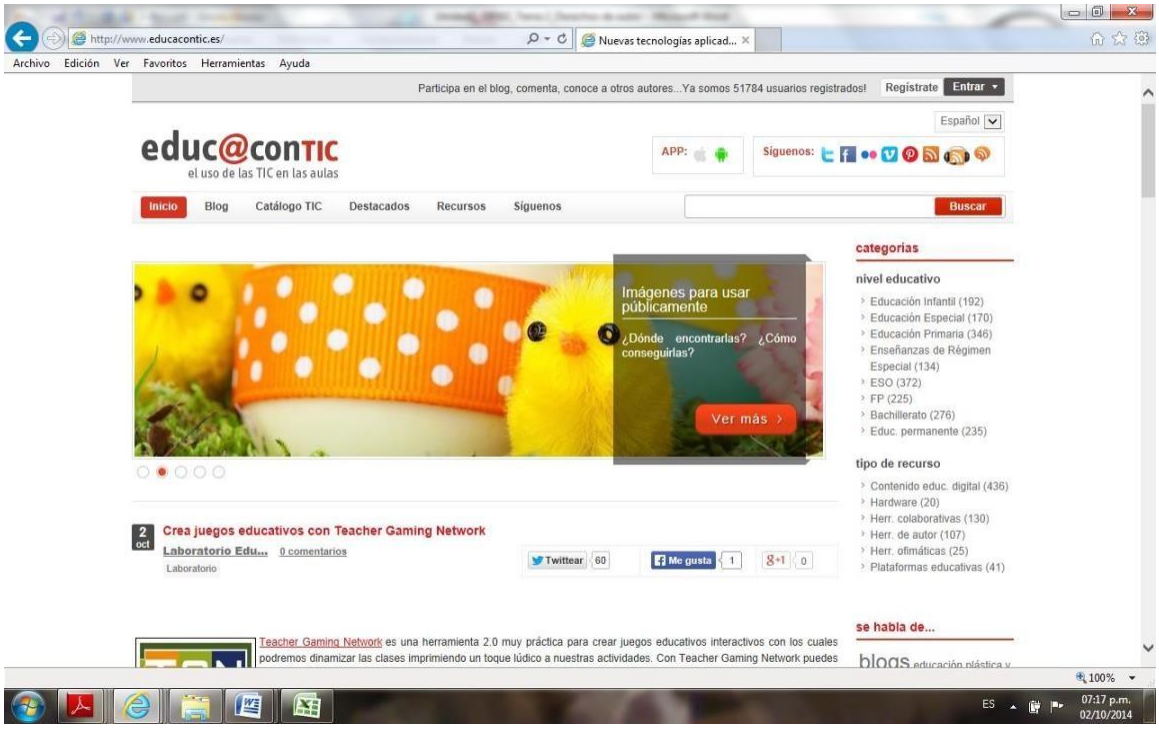
Los recursos web se refieren a que el sitio debe tener propiedad intelectual o el derecho de autor sobre la originalidad de la animación, videos, sonidos, programación del lado del cliente o servidor, lo cual se indica la siguiente figura.



Ejemplo para crear un sitio web (NorfiPC, 2014)

En lo que respecta al contenido del derecho de autor, éste se divide en (García, 2007):

- **Derecho patrimonial:** El creador no recibe remuneración por el video o sitio web.



Ejemplo de sitio donde se exponen herramientas para recursos multimedia sin regalías para el autor (Educa con tic, 2014)

- **Derecho moral:** Se observa cuando el autor recibe un beneficio económico por su creación, ya sea por reproducción o distribución del mismo.

Los derechos de autor en web

Para establecer los derechos de autor en las nuevas tecnologías se han creado convenios internacionales como el establecido en Berna, Suiza, llamado Convenio Berna (García, 2007). Se trata de la aplicación de la ley del país donde se reclama la protección, pero, en el caso de obras con gran componente internacional, como las transmitidas por internet, estableciendo tres posturas distintas:

- Crear un **ciberderecho** como una disciplina que combine el derecho mercantil, el derecho internacional privado y el derecho civil para facilitar una solución global.
- Armonizar las leyes sustantivas mediante tratados internacionales, ya que, al ser la red global, no se pueden tomar soluciones independientes.
- La teoría clásica del conflicto de leyes.

En lo que se refiere a las leyes en relación con el uso de sitios sitio web donde se aloja una obra, la web constituye un lugar de puesta en línea; ante ello, se observa el problema de alojamiento del que nos presta el servicio para publicar nuestro sitio web.

Es importante mencionar que existe un paralelismo entre mundo real y virtual. De esta manera se garantiza la protección efectiva de los autores, pero se generan dos inconvenientes:

- La complejidad al tener que manejar, en teoría, todas las leyes del mundo.
- Posibilidad de diferente calificación jurídica de los actos de explotación y atribución de carácter de autor según el país.

Asimismo, se aclara que en ciertos países se realiza el registro del sitio web. Por ejemplo, en Panamá, la ley del 15 de agosto de 1994 protege la página web, y esto va depender de lo que se requiera registrar. Otro ejemplo es Estados Unidos, donde se deben establecer ciertos criterios para la protección del sitio, como son: registro del sitio, protección de copyright.

Otros aspectos a considerar en la autoría de los sitios web son los siguientes:

- El contenido web.
- El diseño estético y organizacional de la web.
- El código fuente.
- La propuesta de interactividad en el sitio web.

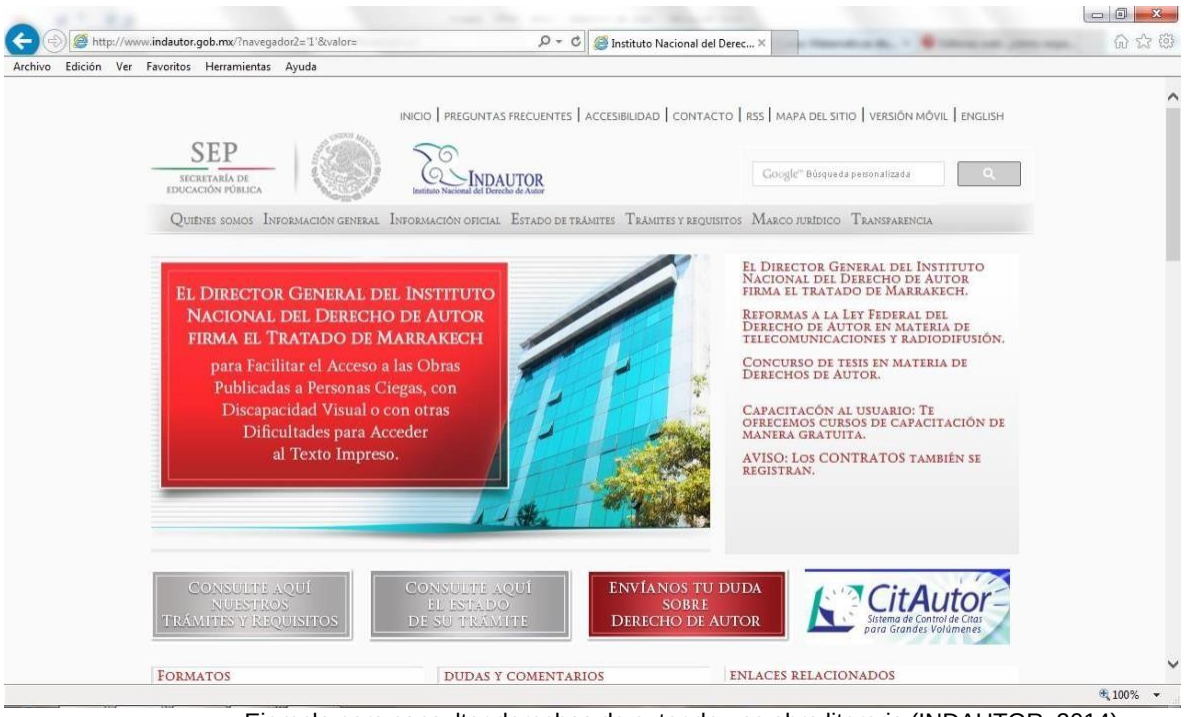
Ejemplo para diseñar web en CC (CC, 2014)

En lo que respecta al diseño web, se evalúan aspectos como una obra literaria, los cuales son:

- Textos con características de una obra literaria
- Imágenes con o sin movimiento

- Audio
- Base de datos para el uso de un diccionario electrónico

Lo anterior lo puedes consultar en el sitio del Instituto Nacional del Derecho de Autor, como lo indica la imagen siguiente:



Ejemplo para consultar derechos de autor de una obra literaria (INDAUTOR, 2014)

2.2. Derechos de autor y protección en Internet

Continuando con el análisis acerca de los elementos que se deben proteger en la web, es importante aclarar que la Dirección General de Derechos de Autor en el México ha establecido criterios para la protección de los datos en internet, estableciendo los siguientes criterios:

- **No protección a las ideas**. El derecho de autor parte de que las ideas son libres y nadie es dueño de ellas, y cuando alguna es novedosa, se protegen; aplicados en Bogotá, Colombia, en el tratado de la Organización Mundial de la Propiedad Intelectual en el año de 1996.
- **Originalidad.** En este aspecto es importante entender que la creación en la web debe incluir información con creatividad, evitando una copia de otra obra; asimismo, se evalúa el esfuerzo del autor para el desarrollo de los contenidos web.

- **No importa el mérito ni la distinción de la obra.** La protección de los datos es independiente del tipo de público al que va dirigida, ya sea científica, cultural o educativa.
- **Ausencia de formalidades para la protección.** Una obra puede recibir el derecho de autor desde su creación.

3. Conexión segura a bases de datos

En la Unidad *1 Tecnologías para mi sitio web*, se enfatizó la necesidad de observar las características de servicio que brindan las empresas de alojamiento web en el caso de que en el sitio web a desarrollar se requiera utilizar una base de datos; es decir, que cuente con conexiones seguras para que, en el caso de que, por ejemplo, se desee realizar negocios en línea, es posible que se necesite solicitar información personal y confidencial, en caso que se inscribieran en un boletín informativo, o en el caso de que realicen un pedido.

Para proteger la información de los clientes es necesario identificar si las empresas de alojamiento web cuentan con el servicio. Es necesario observar que el alojamiento brinde el servicio de SSL, es decir, se utiliza la tecnología llamada SSL o capa de conexión segura (por sus siglas en inglés, *Secure Sockets Layer*), cuya funcionalidad es encriptar los datos que se transmiten entre un navegador web y un servidor web para distinguir si las direcciones web están protegidas con SSL; éstas inician con **https:** en lugar de http.

Ejemplo de certificado SSL estándar GlobalSign (1996)

Esta tecnología es utilizada ampliamente en bancos, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas. No todos los sitios web usan SSL, por eso debes ser cuidadoso (Ramírez y Espinosa, 2011).

El servicio HTTP trabaja con una clave de sesión (que los navegadores piden como excepción) que se negocia en un **handshake** y que puede ser una contraseña de 128 bits; este **handshake** se describe más adelante.

El servicio SSL es la Capa de Conexiones Seguras (por sus siglas en inglés, *Secure Sockets Layer*). Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de internet. Recientemente ha sido sustituido por TLS (*Transport Layer Security*), el cual está basado en SSL, más estas dos tecnologías son totalmente compatibles.

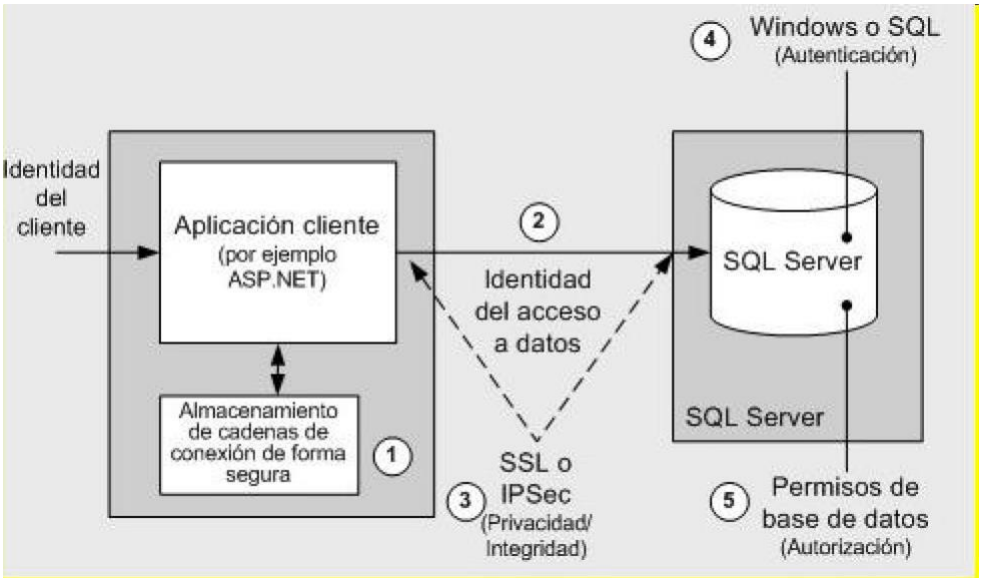
El uso de SSL y/o TLS permite confiar información personal a sitios web, ya que tus datos se ocultan a través de métodos criptográficos mientras navegas en sitios seguros.

La identidad del servidor web seguro.se consigue mediante un certificado digital que comprueba la validez antes de iniciar el intercambio de datos sensibles (Autenticación), mientras que de la integridad de los datos intercambiados se encarga la firma digital mediante funciones hash, así como la comprobación de los resúmenes de los datos enviados y recibidos.

TSL “fue diseñado especialmente para **evitar el ataque** de **hombre** del medio, es por esta razón que presenta mucha dificultad para pasar a través de los **proxies**, pues considera a estos justos como un ataque” (Corletti, 2011, p. 283).

Con hombre del medio se refiere al ataque del intermediario o *man-in-the-middle* (MitM), “hombre del medio”, como se lo conoce en inglés, y es un ataque en el cual un ciberdelicuente es capaz de interceptar y modificar los mensajes de dos usuarios sin que éstos se den cuenta (Tecnoseguridad.Net, 2009).

La siguiente imagen muestra los principales problemas de seguridad asociados al acceso a datos:



Principales problemas de seguridad del acceso a datos (Meier, Mackman, Dunner y Vasireddy, 2003)

A continuación, se enlistan los principales problemas de acceso a los datos en conexiones web de forma segura, según Meier, *Et. al.* (2003).

1. Almacenar cadenas de conexión a bases de datos de forma segura. El uso de la seguridad integrada de Windows es una forma más segura de controlar el acceso a la base de datos y, en caso de que el acceso no sea a base de datos por medio de sistemas de la firma Microsoft, es necesario utilizar credenciales explícitas para iniciar la sesión y el acceso debe ser por medio de cadenas y texto sin cifrar.

2. Usar una identidad o identidades de acceso a datos. Es necesario el uso de identidad o identidades apropiadas para tener acceso a la base de datos. Por ejemplo, si la aplicación "utiliza la autenticación de SQL para conectarse a SQL Servidor, o si se conecta a bases de datos que no son de Microsoft, que requieren credenciales explícitas para iniciar la sesión. En estos casos, las cadenas de conexión contienen nombres de usuario y contraseñas de texto sin cifrar" (Meier, Mackman, Dunner y Vasireddy, 2003, p.2).

3. Asegurar datos que se extienden en la red. Un ejemplo para asegurar los datos sería asegurar los datos confidenciales y las credenciales de inicio de sesión.

4. Autenticar llamadores en la base de datos. Es el mecanismo que ya tiene integrado SQL Servidor.

5. Autorizar llamadores en la base de datos. Se refiere a los permisos que se asocian a objetos de base de datos individuales. Pueden asociarse a usuarios, grupos o funciones.

Para que profundices más respecto a los principales problemas de acceso a datos en la web de forma segura, revisa el documento *U2. Seguridad del acceso a datos*, en el apartado *Material para el desarrollo de la asignatura*.

A continuación, se explicará cómo se asegura la información de las bases de datos y las conexiones a las bases de datos mediante la web (Corletti, 2011).

Aseguramiento de la información de una base de datos. Los datos que están almacenados en MySQL se administran en un servidor. Ante ello, no hay ningún archivo de respaldo que se pueda guardar como el MDB de Access, y que simplemente se copie o guarde, y asegurar así los datos que están en la base de datos y la estructura de la base de datos.

MDB es un archivo de base de datos utilizado por Microsoft Access, MBD es el formato propio de acceso a datos, que se basa en el motor de base de datos Access Jet. El acceso también puede importar o vincular a los datos de otras aplicaciones, como Excel, listas de SharePoint, texto, XML, Outlook y HTML. MDB puede ser abierto por compañías como OpenOffice.org, SAS

Institute, Wolfram Mathematica, Softpedia MDB Converter y Microsoft Visual Studio 2010. Para ser leído por otras aplicaciones, los archivos se pueden convertir a los formatos TXT o. CSV, utilizando un convertidor MDB.

Otra forma de guardar un respaldo y asegurar los datos de forma simple, es copiar el directorio en el que se archivan los datos de la base de datos. En este caso, un ejemplo en MySQL para almacenar una copia de seguridad, se explica a continuación enlistando los pasos:

1. Se copia el subdirectorio DATA de la instalación MySQL en un medio o dispositivo de seguridad, como puede ser otro disco duro. Esto sólo funciona si se tiene acceso al sistema de datos de la computadora en donde se está instalando MySQL, siendo este el método más adecuado, en cualquier caso, para la seguridad de la base de datos en el servidor del proveedor de alojamiento web.

En el caso de que sea por medio del propio servidor de alojamiento web, se realiza creando un extracto de la base de datos, es decir, un **Dump**[1] que se pueda leer después de nuevo en cualquier momento. Normalmente, los proveedores de alojamiento web ofrecen una herramienta para administrar la base de datos que es PhpMyAdmin.

Un **dump** para la aplicación que se utiliza en MySQL; “es un archivo de texto que contiene una serie de sentencias SQL que permiten crear la estructura de una base de datos y cargarla con ciertos datos. Básicamente es una forma de hacer un *backup* (copia) de seguridad portable de una base de datos” (Williams, 2013, p.221).

Si hay que crear un Dump de MySQL en el ordenador local entre el directorio **bin** del directorio de MySQL como ejemplo, se ingresa la instrucción con la siguiente sintaxis.

```
mysqldump –u root Nombrebasededatos > Nombrearchivo
```

En donde:

Com Nombrebasededatos: Indica el nombre de la base datos que se desea asegurar

Nombrearchivo: Se refiere al nombre del archivo en el que debe describirse el dispositivo de seguridad. Es importante no integrar ninguna ruta delante del nombre del archivo; éste se debe crear en el directorio **bin**.

[1] Se suele nombrar como Dump “a la exportación de los datos, así como el archivo que contiene los datos exportados” (Deléglise, 2013, p. 131)

Estructura de directorios MySql, tomado de (http://www.rinconastur.com/php/php8.php)

Root: Es el nombre que se le da al usuario por default y el que realiza el proceso de seguridad; y se le debe asignar una contraseña para el acceso a la base de datos. En la siguiente línea de código se muestra cómo se crea el usuario **root** con su respectiva contraseña.

```
mysqldump –u root –password=Contraseña Nomrebasededatos >Nombrearchivo
```

En este ejemplo hay que observar que se tiene que indicar la contraseña para el usuario **root**, disponible según los derechos correspondientes, para asegurar la base de datos. También se debe indicar el nombre del archivo con la ruta completa (Spona, 2010, p.118-119). Con esta línea que se anexa en la configuración, es posible mantener la información segura en la base de datos.

Para realizar la conexión de la base de datos, y que ésta sea de forma segura, se requiere utilizar el código PHP ejecutado en el sitio web. De esta manera las bases de datos pueden ser gestionadas directamente a través de phpMyAdmin.

PHP Data Objects PDO es una extensión que contiene PHP que utiliza controladores para acceder a datos y motores de base de datos diversos como MySQL, PostgreSQL, Microsoft SQL Servidor, Oracle, etcétera. Proveen una capa de extensión de datos con la cual la codificación depende menos de la base de datos que estemos utilizando debido a que los métodos tienen el mismo nombre para todas las bases de datos que soporta, es decir, ya no es necesario escribir mysql_query para ejecutar una sentencia SQL en MySQL, y cuando se migre a PosgreSQL, ya no se tendrá que cambiar a pg_query.

PDO está disponible desde PHP 5.1 y requiere las nuevas características de programación orientada a objetos que viene desde PHP 5, por lo que no corre en versiones anteriores (Capuñay, 2013, p. 168).

Pasos para realizar la conexión segura a bases de datos mediante PDO. Las conexiones se establecen creando instancias de la clase base PDO (por sus siglas en inglés, *PHP Data Objects*). No importa el controlador que se utilice; siempre se deberá utilizar el nombre de la clase PDO. El constructor acepta parámetros para especificar el origen de datos (conocido como DSN) y, opcionalmente, el nombre de usuario y la contraseña (si la hubiera).

A continuación, se exponen algunos ejemplos de conexión segura a bases de datos mediante PDO:

Ejemplo de conexión a MySQL

```
<?php
$gbd = new PDO('mysql:host=localhost;dbname=test', $usuario,
$contraseña);
?>
```

En este ejemplo, el nombre de la base de datos es **test**. Una vez realizada con éxito una conexión a la base de datos, será devuelta una instancia de la clase PDO al script. La conexión permanecerá activa durante el tiempo de vida del objeto PDO. Para cerrar la conexión, es necesario destruir el objeto, asegurándose de que todas las referencias a él existentes sean eliminadas (esto se puede hacer asignando NULL a la variable que contiene el objeto). Si no se realiza explícitamente, PHP cerrará automáticamente la conexión cuando el script finalice.

Ejemplo 2: Cerrar una conexión:

```
<?php
$gbd = new PDO('mysql:host=localhost;dbname=test', $usuario,
$contraseña);
// Use la conexión aquí

// ya se ha terminado; la cerramos
$gbd = null;
?>
```

Mediante el código anterior se ha creado con el **new** una **instancia** de clase **PDO** (lo que permitirá utilizar varias conexiones a la vez), se define el tipo de base de datos con **mysql,** el servidor se toma como **localhost** (en este caso), el nombre de la base de datos es **dbname=test**, y después, utilizando variables el usuario y la contraseña del servidor de bases de datos.

A continuación, se explicará un ejemplo de conexión normal a una base de datos con PHP.

```
<?php
```

```
$conexion = mysql_connect('localhost', 'usuario', 'contraseña') or
die('Could not connect: ' . mysql_error());
mysql_select_db('bd', $conexion);
$sql = mysql_query("SELECT * from usuarios");
while($columna = mysql_fetch_array($sql)){
    echo $columna["Nombre"];
?>
```

Esta conexión podría ser **hackeable**, por ello, en PDO se realiza la conexión de una forma diferente pero con mayor seguridad, utilizando el método **prepared statements**, con el fin de que la conexión a la base de datos por medio de internet sea más difícil de acceder. Esto se hace de la siguiente forma:

```
1. <?php
2. $nombre = "Juan";
3. try{
4. $conn = new PDO('mysql:host=localhost;dbname=basededatos', $usuario,
$contra);
5. $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
6. $sql = $conn->prepare('SELECT * FROM usuarios WHERE nombre =
:Nombre');
7.      $sql->execute(array('Nombre' => $nombre));
8.      $resultado = $sql->fetchAll();
9. foreach ($resultado as $row) {
10. echo $row["Id"];
11. }
12. }catch(PDOException $e){
13.      echo "ERROR: " . $e->getMessage();
14. }
15. ?>
```

Método prepare

Se hace la conexión a la base de daos

Devuelve los datos de la consulta

Imprime el resultado de la consulta

En el código anterior, en primer lugar, se utiliza el método **prepare**, de la función **conn**, y se le pasa la consulta como parámetro; puede ser cualquier consulta SQL, no hace falta que sea tan sencilla como la que se expone en el ejemplo, pero donde se agrega la variable "**Nombre"**, definida antes, se vuelve a utilizar **":Nombre",** pero se le pasa la misma variable como parámetro en un **array** dentro del **execute** en la línea siguiente (la línea 8). Posteriormente se agrega un **fetch** para que devuelva los datos de la consulta para, finalmente, concluir con un **foreach** que muestra el resultado.

Hay varias formas de utilizar **fetch**. En el caso de que no se le pase ningún parámetro, regresará un **array**. De igual forma, se puede definir para que regrese una instancia de clase o un objeto.

Según PHP.NET (2014), los diferentes parámetros a tomar en cuenta son:

PDO::FETCH_ASSOC: Este parámetro regresa un **array** indexado por los nombres de las columnas del conjunto de resultados.

PDO::FETCH_BOTH (predeterminado): Este parámetro devuelve un **array** indexado tanto por nombre de columna como numéricamente con índice de base 0.

PDO::FETCH_BOUND: Regresa **true** y asigna los valores de las columnas del conjunto de resultados a las variables de PHP a las que fueron vinculadas con el método **PDOStatement::bindColumn()**.
PDO::FETCH_CLASS: Devuelve una nueva instancia de la clase solicitada, haciendo corresponder las columnas del conjunto de resultados con los nombres de las propiedades de la clase.

El método **prepared statements**, explicado en el ejemplo anterior, es el más conveniente y de conexiones seguras para acceder a bases de datos MySQL. Algunas de sus características y ventajas son:

- Interfaz más elegante, basado en objetos.
- Compatibilidad con diversos motores de bases de datos, no sólo MySQL.
- Mayor seguridad a la hora de construir consultas SQL.
- Compatibilidad con herramientas avanzadas de bases de datos: procedimientos almacenados, transacciones, sentencias preparadas.
- Mejor rendimiento y optimización frente a las funciones clásicas de PHP.
- Gestión de errores más conveniente.

Conexiones seguras con handshake. Es el proceso de **intercambio de información privada**. Cuando un usuario entra en una página web para intercambiar información, y ésta, a su vez, es privada, con **SSL** o protocolo **https**, se ejecuta un proceso llamado popularmente *handshake*.

Según el sitio el protocolo TLS, está diseñado para asegurar y autenticar la comunicación a través de una red pública mediante la codificación de datos. El protocolo de enlace TLS permite que el servidor y el cliente provean autenticación mutua y negocien un algoritmo y claves de codificación antes de transmitir los datos. Para hacer **un handshake** se debe hacer un túnel TLS que se inicia a través de una **conexión normal**, por ejemplo, cuando esta conexión es HTTP, primero se establece una conexión de texto plano y a través del handshake se crea la **conexión segura** por medio del **intercambio** de **claves** y la generación del **secreto compartido**, junto con el código de autenticación del mensaje.

Un túnel TSL se utiliza para conseguir la mayor seguridad al realizar una VPN con OpenVPN se debe utilizar criptografía asimétrica (o de clave pública) (IPC, s/f).

Existen dos formas de llevar a cabo el handshake para iniciar con una conexión TSL:

Handshake completo: Este sirve para iniciar una conexión, lo cual puede no llevar a cabo la autenticación del cliente o el servidor.
A continuación, se expone la secuencia de pasos que componen el **handshake** de la **apertura** de una conexión segura, usando el TLS handshake protocol, en la que aplica el handshake completo (Corletti, 2011).

Paso 1: El cliente le envía al servidor el número de versión de TLS (o bien, de SSL), los cipher que quiere usar, datos generados aleatoriamente, y otros tipos de información que el servidor necesita para comunicarse con el cliente usando TLS.

Paso 2: El servidor le envía al cliente el número de versión del TLS (o SSL) del servidor, los cipher que quiere usar, datos generados aleatoriamente, y otros tipos de información que el cliente necesita para comunicarse con el servidor vía TLS.

Paso 3: El cliente usa parte de la información enviada por el servidor para autenticarlo Si el servidor no puede ser autenticado, se le avisa del problema al usuario y se le informa que no se puede establecer una conexión encriptada y autenticada con ese servidor. Si el servidor puede ser autenticado satisfactoriamente, el cliente avanza hacia el paso 4.

Paso 4: Usando todos los datos generados en el handshake hasta ahora, el cliente (con la cooperación del servidor, y dependiendo del **cipher** siendo usado) crea el **premaster secret** para esta sesión, lo **encripta** con la clave pública del servidor y envía el **premaster secret** encriptado hacia el servidor.

Paso 5: Si el servidor requirió la autenticación del cliente (un paso opcional en el handshake), el cliente también firma (digitalmente) otra pieza de datos que es única a este handshake y conocida por ambas partes. En este caso, el **cliente manda** los datos **firmados** y su propio certificado al servidor, junto con el premaster secret

Paso 6: Si el servidor requirió la autenticación del cliente, el servidor intenta autenticar el cliente. Si el cliente no puede ser autenticado, la sesión es terminada. Si el cliente puede ser satisfactoriamente autenticado, el servidor usa su clave privada para **desencriptar** el **premaster** secret, luego lleva a cabo una serie de cálculos (los cuales el cliente también ejecuta, empezando por el premaster secret) para generar el master secret.

Paso 7: Se detectan los cambios en los datos mientras éstos viajaban por la red, antes de ser recibidos por la conexión TLS.

Paso 8: El cliente envía un mensaje al servidor, informándole que mensajes futuros desde el cliente serán encriptados con la session key. Luego éste manda un mensaje (encriptado) separado indicando que la parte cliente del **handshake** ha terminado.

Paso 9: El servidor manda un mensaje hacia el cliente, informándole que los futuros mensajes desde el servidor serán encriptados con la session key (para detalles, ver change cipher spec Protocol). Luego éste manda un mensaje (encriptado) separado, indicando que la parte servidor del handshake ha terminado.

Paso 10: En este momento, el handshake TLS está completo, y la sesión TLS ha empezado. El cliente y el servidor usan las session keys para encriptar y desencriptar los datos que se mandan uno con otro y para validar su integridad.

Handshake abreviado: Se utiliza para reanudar una conexión previa que se mantiene en el cache del servidor y sólo se verifican los parámetros del **ciphersuite** (protocolo de intercambio de especificaciones de cifrado) a utilizar. A continuación se explica el handshake abreviado.

El cliente envía un **ClientHello** usando el **session-ID** de la sesión a ser reanudada y otros 48 bytes **random**. El servidor luego chequea en su **cache** de sesiones para ver si encuentra esa sesión. Si se encuentra la sesión, y el servidor está dispuesto a restablecer la conexión bajo el estado especificado de sesión, mandará un ServerHello con el mismo valor de **session-ID** y otros 48 bytes random. Se debe regenerar el **master secret** y las claves de sesión, los secretos MAC y los IVs. En este punto tanto el cliente como el servidor deben enviar directamente mensajes ChangeCipherSpec y Finished. Una vez que el restablecimiento está completo, el cliente y servidor empiezan a intercambiar datos de aplicación.

Si el servidor no puede encontrar el **session**-ID en su cache, el servidor genera una nuevo **session-ID** y tanto el cliente como el servidor TLS ejecutan un **handshake** completo.

Mensajes para la conexión con handshale abreviado	
Cliente	Servidor
ClientHello	
	ServerHello
	ChangeCipherSpec
	Finished
ChangeCipherSpec	
Finished	
Datos de Aplicación < ---->	< ----> Datos de Aplicación

Ejemplo de mensajes para la conexión con handshake abreviado (Corletti, 2011)

Las fases de handshake son tres y se describen a continuación:

1. Se negocian los algoritmos

- Algoritmo de cifrado simétrico y asimétrico
- Método de intercambio de claves
- Funciones resumen

2. Autenticación del servidor (obligatoria). Opcionalmente se autentica al cliente

3. Se genera el secreto compartido.

```
master_secret basado en el intercambio DH denominado
pre_master_secret.
master_secret = hash (pre_master_secret|N_cliente|N_servidor)
```

La seguridad es un aspecto importante y fundamental para muchas aplicaciones cliente-servidor, siendo un ejemplo muy importante, por su gran proyección en los últimos tiempos, el negocio electrónico.

Mediante el uso de handshake SSL/TLS se ha conseguido aumentar el grado de seguridad en dichas conexiones cliente-servidor. Handshake se compone de tres sub-protocolos que se utilizan para permitir que los puntos de acuerdo en los parámetros de seguridad de la capa de registro, autenticación de sí mismos, crear instancias de los parámetros de seguridad negociados, y reportar las condiciones de error. Este protocolo es responsable de negociar una sesión segura.

Para saber más

Se te recomienda investigar más sobre el tema de seguridad y visibilidad de un sitio web, visitando los siguientes sitios:

- http://googlewebmaster-es.blogspot.mx/2011/07/seguridad-en-sitios-web-para-webmasters.html
- http://googlewebmaster-es.blogspot.mx/2008/11/gua-seo-de-google-para-principiantes.html
- https://support.google.com/webmasters/answer/35769

Para saber más sobre la propiedad intelectual es recomendable que consultes el siguiente sitio: https://www.flacso.edu.ec/

Para saber más sobre Dump, es recomendable que revises los siguientes sitios:

- http://douglasfloresnic.blogspot.mx/2010/06/script-php-para-hacer-respaldo-de.html

- Williams, P. (2013). *Sistema de gestión de una distribuidora*. Montevideo: Universidad ORT Uruguay.
- IPC Institut Puig Castellar (s/f). *Actividad 3: Túnel SSL/TLS*.
- Tecnoseguridad. NET (2009). *Cómo protegernos del ataque del hombre en el medio o intermediario.* Disponible en https://blog.segu-info.com.ar/2009/02/como- protegernos-del-ataque-del-hombre.html

Cierre

La seguridad de un sitio web es de suma importancia, y no es posible dejar de considerarla en la creación y modificación de páginas web, sobre todo si se desea ganar la confianza de los prospectos o clientes potenciales. Para ello, es indispensable que conozcas las formas de aplicar seguridad a las páginas web.

Por otro lado, la visibilidad de un sitio web también es de gran relevancia si se desea llegar a más clientes potenciales. Hoy en día se cuenta con muchas formas de hacer visible una página web; únicamente hay que conocer esas formas y elegir la que más convenga a los intereses de la empresa que se desea promover.

La importancia de los derechos de autor consiste en saber cómo utilizar o cuándo utilizar recursos, sitios, contenidos etcétera, que están registrados y cuentan con un derecho de autor, así como saber los lineamientos de la web y una obra literaria. Su importancia se ubica en el repunte comercial que día con día tienen las páginas web, ante lo cual es importante considerar los cauces legales que se deben seguir al desarrollar un sitio web y los recursos que es posible dar a conocer al mundo mediante estos sitios.

En esta unidad se explicaron las características principales para considerar al momento de realizar una conexión a la base de datos de un sitio que se encuentra alojada en un servidor web, así como ejemplos de conexiones diferentes para observar los tipos de seguridad en conexiones; esto con la finalidad de que puedas realizar transacciones seguras en el sitio web y mantener segura la información correspondiente.

Fuentes de consulta

- Arced, C. y Arqués (18 de marzo, 2010). *Visibilidad: cómo gestionar la reputación en internet*.
- BIBLIOSEO (2012). *¿Qué es la visibilidad web y por qué es importante en las bibliotecas?* Disponible en http://www.biblioseo.com/2010/04/que-es-la-visibilidad-web-y-por-que-es.html#ixzz3JfitkCyr
- Capuñay, O. (2013). *Desarrollo Web con PHP: Aprende PHP paso a paso*. (N.D.)
- Corletti, E. A (2011). *Seguridad por niveles*. Madrid, Creative Commons
- Cv.uoc.edu. (2019). *Reputación digital*. [online]. Disponible en https://n9.cl/jcyh1
- Deleglise, D. (2013). *MySQL 5 (Versiones 5.1 a 5.6). Guía de referencia del desarrollador.* Barcelona: Ediciones ENI.
- DNDA Dirección Nacional del Derecho de Autor (2014). *Preguntas frecuentes*.
- Flores, A. (2014). Procesamiento y análisis de datos. Disponible en https://prezi.com/2s1alavuskd_/copy-of-procesamiento-y-analisis-de-datos/
- García García, J., y Martínez, I. de J. *Protección de los derechos de autor en Internet: Los derechos de autor en el entorno digital*. Disponible en http://www.rinconcastellano.com/trabajos/copiaprivada/3_internet.html#
- García Gómez, F. J. (10 de octubre, 2009). *Posicionamiento y visibilidad web de las bibliotecas públicas españolas: situación actual y estrategias de desarrollo.* Disponible en http://travesia.mcu.es/portalnb/jspui/bitstream/10421/696/1/com_426.pdf
- García Heredia, A. (2007). *Los cánones: Derechos de autor, propiedad industrial y Know How*. España: Editorial Lex Nova.
- Garfinkel, S. (1999). *Architects of the Information Society*. Massachusetts: Massachusetts Institute of Technology.
- Herrera Meza, J.H. (1992). *Iniciación al Derecho de Autor*. México: Limusa Grupo Noriega Editores.

- INDAUTOR Instituto Nacional del derecho de autor (2014). *Preguntas frecuentes*.

- Kioskea.NET (2014). *Editores web: ¿cómo respetar los derechos de autor?* Disponible en https://es.ccm.net/faq/8855-editores-web-como-respetar-los-derechos-de-autor

- López, C., y Estrada, A. (2007). *La protección de las publicaciones en el contexto. En: Edición y derechos de autor en las publicaciones de la UNAM*. México: UNAM DGSCA Publicaciones digitales.

- Meier, J.D., Mackman, A., Dunner, M., y Vasireddy, S. (2003). *De la seguridad del acceso a datos en aplicaciones ASP .NET.*

- Morales, E. (2011). *Registro de diseño de páginas web en la Ley Federal del Derecho de Autor.* Tesis (Licenciatura en derecho). Disponible en http://132.248.9.195/ptb2011/junio/0669692/Index.html

- MSDN Microsoft System Development Network. (2014). *Documentación de Microsoft, Autorización y autenticación.* Disponible en http://msdn.microsoft.com/es-es/library/ms457529(v=office.12).aspx

- Nolasco Ramírez, Y. (2005). Régimen fiscal de los derechos de autor. Tesis (Licenciatura en Derecho con área en Derecho Fiscal). Disponible en http://catarina.udlap.mx/u_dl_a/tales/documentos/lfis/nolasco_r_y/capitulo2.pdf

- OWASP (2014). *Validación de entradas: Input Validation Cheat Sheet.* Disponible en https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet

- PHP.NET (2014). *PDOStatement::fetch*. Disponible en https://www.php.net/manual/es/pdostatement.fetch.php

- Prat, M. (2013). *SEO Posicionamiento de su sitio web: en Google y otros buscadores*. 3ª Edición. Barcelona: ENI Ediciones.

- Ramírez, D.O., Espinosa, C.C. (3 de mayo del 2011). El Cifrado Web (SSL/TLS). *Revista Seguridad cultura de prevención para TI*. No.10 p.1. México: UNAMCERT-DGTI. Disponible en https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

- Rincón, E. (2006). *Manual de derecho de comercio electrónico y de internet.* Bogotá: Universidad del Rosario.

- Spona, H. (2013). *Programación de bases de datos con MYSQL y PHP*. Barcelona: Marcombo.
- Téllez Valdés, J. (2004). *Derecho informático*. México: McGraw Hill.
- Triana Bohórquez, I.E. (13 de octubre del 2012). *Con la tecnología de Blogger*. Disponible en http://www.biblioseo.com/2010/04/que-es-la-visibilidad-web-y-por-que-%20es.html#ixzz3JfjJI7Dh
- UDB Universidad Don Bosco (2014). 2*. Formularios web y controles de validación.*
- UNAM-CERT (2014). *Sugerencias de Seguridad para Sitios Web*. UNAM: Coordinación de Seguridad de la Información. Disponible en http://www.seguridad.unam.mx/documento/?id=1143Definición de vulnerabilidad - Qué es, Significado y Concepto http://definicion.de/vulnerabilidad/#ixzz3HVLVi81Y
- UNAM-CERT (2014). Sugerencias de Seguridad para Sitios Web. UNAM: Coordinación de Seguridad de la Información. Recuperado de http://www.seguridad.unam.mx/documento/?id=1143Definición de vulnerabilidad - Qué es, Significado y Concepto http://definicion.de/vulnerabilidad/#ixzz3HVLVi81Y
- Unijimpe (2011). *Manejo de sesiones en PHP*. Disponible en http://blog.unijimpe.net/manejo-de-sesiones-en-php/
- Ventura, V. (9 de noviembre, 2011). *Cómo ganar visibilidad en internet*. Disponible en https://www.emprenderalia.com/como-ganar-visibilidad-en-internet/

Bibliografía complementaria

- Peñeñory, V.M. (s/f). *Derechos de autor para medios electrónicos*. Disponible en https://www.slideshare.net/vmpenenori/clase-7-1452998
- Quintanilla Mendoza, G. (s/f). *Los derechos reservados en la Web.* Disponible en http://www.revista.unam.mx/biblioteca/mastergabriela.pps

Fuentes de imagen

- CC Creative Commons (2014). *¿Eres un Creative Commoner y te interesa promover tu trabajo?* Disponible en https://creativecommons.org/licenses/?lang=es
- Educa con tic (2014). *Uso de las TIC en las aulas*. Disponible en http://www.educacontic.es/
- GlobalSign (1996). *Centro de Información SSL*.
- INDAUTOR Instituto Nacional de Derechos de Autor (2014). *El director General del Instituto Nacional del Derecho de Autor firma el tratado de Marrakech para facilitar el acceso a l*
- Instalación de MySql (s/f) *Estructura de directorios MySql.* Disponible en https://manuales.guebs.com/mysql-5.0/installing.html
- NorfiPC (2014). *Creación, edición de páginas web, estilo y diseño web*. Disponible en http://norfipc.com/web/
- Willy.net (2008). *De la Seguridad del acceso a datos en aplicaciones ASP NET*.