DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Jornadas de
Visibilidad Web UNAM 2022

Consideraciones que no deben faltar en la implementación de un sitio web

Mario Alberto Arredondo G.

Visibilidad Web UNAM

Sitios web implementados con…

- Servidores dedicados
- Contenedores
- Máquinas virtuales
- Diferentes Sistemas operativos
- Lenguajes de programación
- Servidor Web
  - Apache
  - Nginx
- Base de datos
  - MySQL
  - MariaDB
  - PostgreSQL
- CMS
  - Wordpress
  - Drupal
  - Joomla

Consideraciones en la implementación de un sitio web

Se trata de una aproximación a una **lista mínima de elementos a considerar** para la publicación de sitios web.

Tomando en cuenta diferentes capas o niveles, como la **infraestructura**, el **software** y hasta **políticas de uso y buenas prácticas**, involucrando a varios perfiles que intervienen en la publicación de un sitio Web.

Algunas consideraciones en cuanto a la seguridad

- Uso de contraseñas seguras
- Cambiar el nombre del usuario administrador por defecto
- Validar las entradas de los formularios
- Usar CAPTCHA para formularios
- Usar certificados SSL, TLS y protocolo HTTPS
- Actualizar la plataforma de publicación
- Restringir el acceso a archivos y directorios
- Evaluar la implementación de un WAF
- Desactivar módulos o plugins que no se usen
- Crear copias de seguridad

Uso de contraseñas seguras (i)

- Se recomienda controlar el primer acceso al sistema con una contraseña segura.
- Establecer contraseñas de 8 a 12 caracteres (como mínimo).
- Combinar números, símbolos, letras en mayúsculas y minúsculas.
- El sistema debe verificar la existencia de estos elementos al modificar o crear una nueva contraseña de usuario
- Sugerir a los usuarios evitar combinaciones obvias, secuencias de números continuos, palabras conocidas o asociadas al usuario.
- Contemplar el uso de autenticación en dos factores.
- Es recomendable limitar el número de intentos de acceso para reducir la posibilidad de ataques de terceros.

Uso de contraseñas seguras (ii)

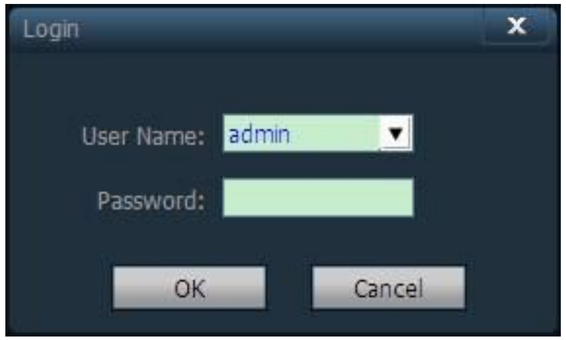
Evitar usar…

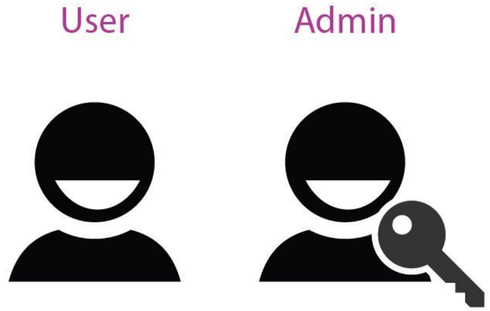
Posición	2017	2018	2019	2020	2021
1	123456	123456	12345	123456	123456
2	password	password	123456	123456789	123456789
3	12345678	123456789	123456789	picture1	12345
4	qwerty	12345678	test1	password	qwerty
5	12345	12345	password	12345678	password

Reporte que realiza NordPass todos los años acerca de las 200 contraseñas más elegidas por los usuarios, se analizó una base de datos de 4TB con contraseñas de usuarios de 50 países recopiladas.

Cambiar el nombre del usuario administrador por defecto

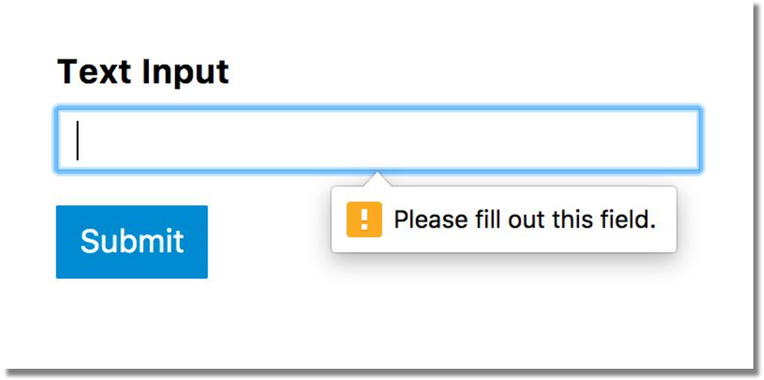
- Si se utilizan Sistemas de Gestión de Contenidos (CMS por sus siglas en inglés, *Content Management System*), es altamente recomendable **cambiar el nombre del usuario administrador** que viene por defecto; con la intención de mitigar un posible ataque utilizando un nombre de usuario conocido.





Validar las entradas de los formularios (i)

- Este tipo de validaciones son una **primera barrera para evitar ataques**, por ejemplo de SQL *Injection* o XSS (*Cross-Site Scripting*).
- Una **primera capa de validación** podría implementarse desde el navegador del usuario, antes de enviar la información al servidor.
- Siempre **es necesario realizar esta práctica del lado del servidor** porque no es posible tener control de la procedencia de los datos o del navegador de usuario.



Validar las entradas de los formularios (ii)

Por ejemplo un ataque XSS

```
// Nombre del usuario registrado
echo "Nombre: " . $_GET["query"];
// Mensaje de éxito de registro
//código...
```

registro.php

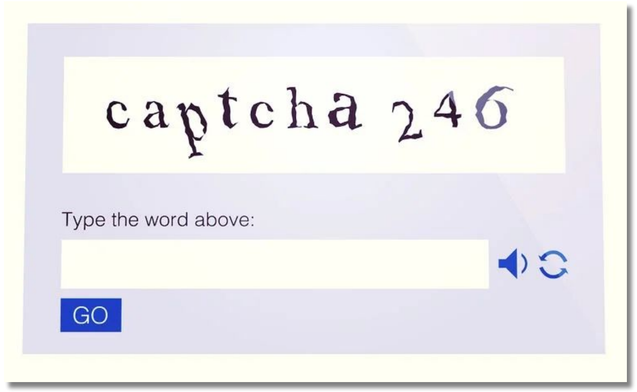
El problema es que la variable **$_GET["query"]** no es validada o escapada, por lo que un atacante podría enviar el siguiente link a la víctima.

http://misitio.com/registro.php?query=<script>alert("hackeado")</script>

Usar CAPTCHA para formularios (i)

El CAPTCHA es una medida de seguridad “pregunta-respuesta” que **ayuda a proteger las entradas del sistema** de posible *spam* y del descifrado de contraseñas, solicitando al usuario demuestre que es un ser humano, no una computadora (robot) tratando de acceder.

Existen diferentes opciones para el uso de CAPTCHA en un sistema que se pueden utilizar en desarrollos propios “a medida” y en diferentes sistemas administradores de contenido.



Usar CAPTCHA para formularios (ii)

Para implementar reCAPTCHA en un sistema diseñado a la medida, se puede consultar la documentación del lenguaje o *framework* utilizado pues cada uno tiene sus propios métodos.

Si se trata de un CMS, como WordPress o Drupal, existen plugins o módulos que facilitan la configuración del CAPTCHA o reCAPTCHA.

WordPress

- **reCaptcha**; https://es.wordpress.org/plugins/google-captcha/
- **Advanced Google reCAPTCHA**: https://es.wordpress.org/plugins/advanced-google-recaptcha/
- **Really Simple CAPTCHA**: https://es.wordpress.org/plugins/really-simple-captcha/

Drupal

- **CAPTCHA**: https://www.drupal.org/project/captcha
- **reCAPTCHA v3**: https://www.drupal.org/project/recaptcha_v3

Usar certificados SSL y protocolo HTTPS

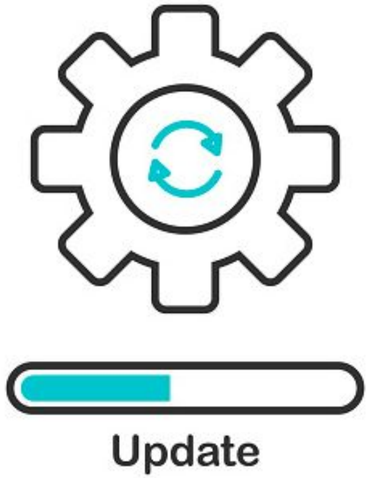
El protocolo HTTPS (*Hyper Text Transfer Protocol Secure*) o **protocolo seguro de transferencia de hipertexto** permite una conexión segura entre el servidor web y el navegador. Para usar el protocolo HTTPS en un sitio web **es necesario adquirir un certificado digital SSL**, éste autentica la identidad de un sitio web y habilita la conexión cifrada.

Nota: En la UNAM se pueden obtener los certificados de seguridad SSL a través del área de Firma Electrónica Avanzada (FEA), un servicio que se ofrece a través de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). *https://www.fea.unam.mx/SSL*

Actualizar la plataforma de publicación (i)

Para contemplar mejoras de **seguridad**, así como de **rendimiento** y **desempeño** en las aplicaciones web.

- Software del servidor
- Gestor de contenidos



Actualizar la plataforma de publicación (ii)

Infraestructura del servidor

Es necesario actualizar las versiones de este software para mejorar su compatibilidad, tener acceso a parches que remedien problemas de seguridad conocidos y aprovechar mejor los recursos de hardware disponibles.

Gestor de contenidos

Actualizar el gestor de contenidos utilizado en un sitio web es de vital importancia para **obtener nuevas funcionalidades**, **mejorar la usabilidad y experiencia del usuario**, **optimizar el rendimiento** y **atender riesgos en materia de seguridad** de la información.

Actualizar la plataforma de publicación (iii)

En el proceso de actualización se deben tomar en cuenta los siguientes puntos:

- Comprobar la **compatibilidad** de los elementos a actualizar: plugins, módulos, plantillas, temas gráficos, entre otros.
- Activar el “modo de mantenimiento” para **informar a los usuarios** que el sitio se encuentra en una fase de actualización.
- Crear copias de seguridad. Es necesario **contar con un respaldo actualizado** del sitio para recuperar la información, en caso de alguna falla.

Restringir el acceso a archivos y directorios (i)

Un aspecto básico de seguridad es **proteger el listado de archivos** contenidos en los directorios públicos de un servidor web, ya que podrían contener **información importante** respecto al servidor como configuraciones o versiones de software utilizadas.

Restringir el acceso a archivos y directorios (ii)

Algunas opciones para restringir el acceso:

Archivo index.html
Para algunos casos incluir un archivo **index.html** en cada directorio del sitio es suficiente para evitar que se muestre su contenido y solucionar el problema.

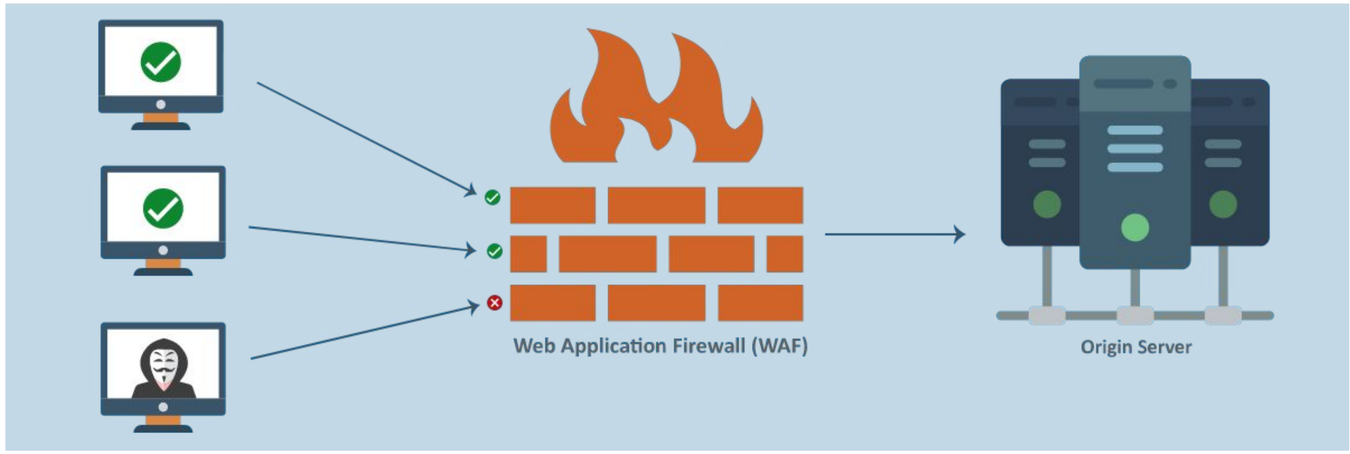
Archivo .htaccess
Si se usa un servidor web Apache, se puede agregar una directiva que evite que se desplieguen los archivos de los directorios de publicación web. Esto se logra creando un archivo ***.htaccess*** en la raíz del sitio web o agregando, si ya se cuenta con uno, la siguiente directiva: ***Options - Indexes***

Archivo de configuración de Apache (httpd.conf)
Si utilizamos, ***Options -FollowSymLinks*** y no utilizamos la directiva *Indexes*, no se mostrará nada y nos mostrará acceso prohibido “*Forbidden*“.

Evaluar la implementación de un WAF

Un WAF (*Web Application Firewall*) **protege a las aplicaciones web** de posibles ataques de XSS (*Cross - Site - Scripting*), SQL Injection, envenenamiento de cookies y algunos otros, desde la capa de la aplicación.

Su adopción puede evitar que terceros tengan acceso a los datos sin autorización.



Desactivar módulos o plugins que no se usen

En el caso de que la publicación del sitio web sea a través de un CMS, **es altamente recomendable** desactivar los módulos o plugins que no se estén utilizando o que se hayan utilizado mientras se construía el sitio.

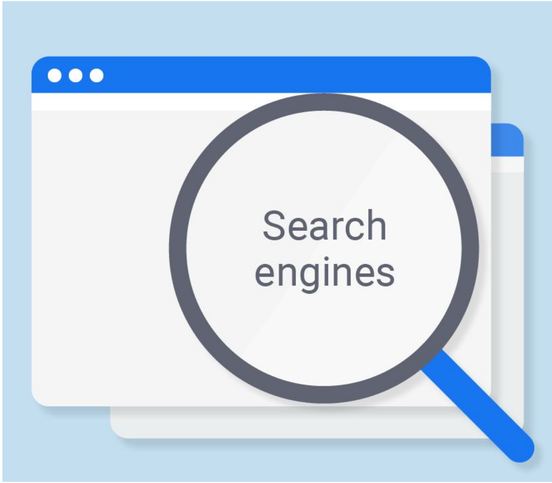
Crear copias de seguridad

Es necesario **establecer una política** en cuanto a la creación de copias de seguridad del sitio.

La creación de copias de seguridad (backup) pueden permitir que el sitio se restablezca desde un punto en el tiempo cercano a una posible falla, **minimizando así la pérdida de información** y permitiendo la restauración del sitio.

Algunas consideraciones en cuanto a la visibilidad

- Uso de URL amigables o semánticas
- Uso las etiquetas H1, H2 y H3 para los encabezamientos
- Verificar las opciones de configuración
- Crear el sitemap del sitio
- Agregar el sitio a Google Search Console
- Módulos y plugins para CMS



Uso de URL amigables o semánticas

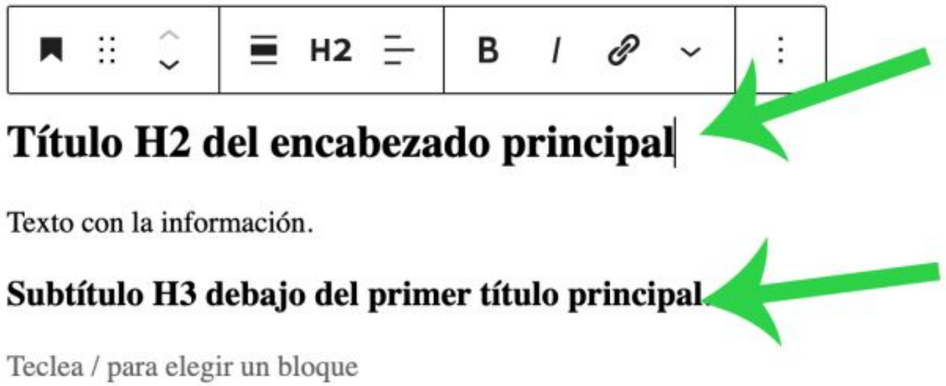
Los enlaces permanentes se forman por una dirección **URL que pertenece al dominio del sitio web**, **una ruta de directorio** necesario en caso de especificar una categoría o agrupación para la página y una **cadena que identifica el recurso específico**, algo fundamental para el adecuado posicionamiento e indexación de la página en los motores de búsqueda.

Para la página: 

Dominio del sitio: ***www.visibilidadweb.unam.mx***
Ruta o directorio específico: ***buenas-practicas***
Cadena que identifica la página: ***usabilidad***

Uso las etiquetas H1, H2 y H3 para los encabezamientos

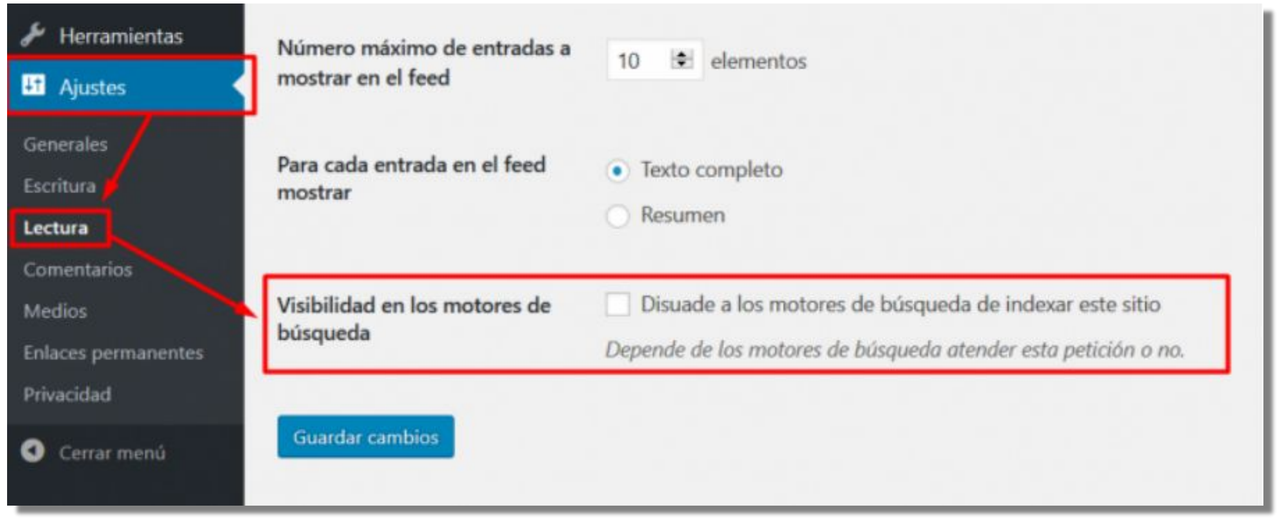
El uso de las etiquetas <h1>, <h2> y <h3> para los encabezamientos principales en el contenido, ayuda a **organizar de manera jerárquica la información** contenida y facilita la lectura para los usuarios, además de que **proporcionan el contexto** de la página a los motores de búsqueda.



Verificar las opciones de configuración

En el caso de utilizar un administrador de contenidos (CMS) como WordPress, es recomendable **verificar la correcta configuración de opciones de publicación**.

Por ejemplo, la opción: "*Disuade a los motores de búsqueda de indexar este sitio*".



Crear el sitemap del sitio

El sitemap es una **lista estructurada de todas las páginas en un sitio web**, incluye la página principal, además de los vínculos hacia archivos o documentos importantes del sitio (archivos PDF, videos, entradas, páginas, etc.)

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="/sitemap_generator/default/si
<!--Generated by the Simple XML Sitemap Drupal module: https://drupa
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9" xmlns:im
 <url>
  <loc>https://www.visibilidadweb.unam.mx/</loc>
  <lastmod>2022-09-14T11:29:51-05:00</lastmod>
  <changefreq>daily</changefreq>
  <priority>1.0</priority>
 </url>
 <url>
  <loc>https://www.visibilidadweb.unam.mx/buenas-practicas</loc>
  <lastmod>2022-09-07T10:35:41-05:00</lastmod>
  <priority>0.5</priority>
 </url>
 <url>
  <loc>https://www.visibilidadweb.unam.mx/buenas-practicas/visibilid
  <lastmod>2022-09-07T10:44:20-05:00</lastmod>
  <priority>0.5</priority>
 </url>
```

https://www.sitemaps.org/es/protocol.html

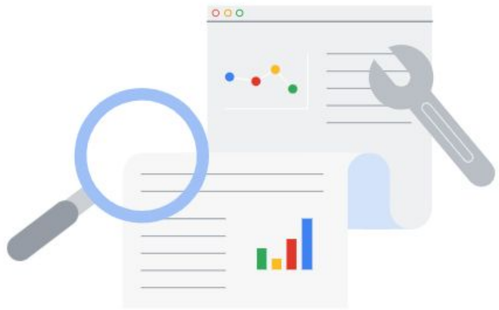
Agregar el sitio a Google Search Console

Google Search Console **ayuda a supervisar y dar solución a posibles problemas con la indexación del sitio** en el motor de búsqueda de Google.

Esta herramienta permite entender y mejorar la manera en que Google ve al sitio web.

Hay que añadir el sitio a Search Console de Google en la URL:

https://search.google.com/search-console/about



Módulos y plugins para CMS

Hacer un **correcto uso de los plugins** que pueden aportar a la adecuada configuración del sitio web.

- **XML Sitemap**
Genera un mapa del sitio en formato XML según el protocolo definido en sitemaps.org.

- Módulo **Meta tag**
Para el uso de meta etiquetas en las páginas de Drupal.

- **Broken Link Checker**
Este plugin monitorea y realiza pruebas de los enlaces internos y externos en las publicaciones, páginas y comentarios de un sitio creado en WordPress, buscando los posibles enlaces rotos e imágenes faltantes.

- **Schema – All In One Schema Rich Snippets**
Facilita la implementación de los datos estructurados.

- **Yoast SEO**
Un plugin gratuito que nos ayudará a mejorar aspectos importantes de la visibilidad web.

DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Gracias

Mario Alberto Arredondo
malag@unam.mx

Visibilidad Web UNAM