GUIA DE ESTANDARIZACION PARA SITIOS WEB EL SALVADOR 2015

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

CONTENIDO

A-1 Política Tecnológica.....3

B.1 Configuración de Seguridad.....5

B.2 Configuración de Acceso.....5

C.1 Diseño Estructural.....8

D.1 Diseño Accesible.....10

E Estándares sobre Contenido.....13

E.1 Contenido estático.....13

E.2 Contenido dinámico.....14

F.1 Funcionalidades.....17

F.2 Uso de Sitio Web.....18

Anexos

A - Estandares sobre politica Tecnologica

A-1 Política Tecnológica

A-1 Política Tecnológica

A.1.1 Hay alguien encargado de atender y contestar el correo electrónico de contacto y los formularios de contacto:
Criterio de puntuación: *0 – No existe. 10 – Existe*

A.1.2 ¿Se cuenta con un plan de respaldo de información para los archivos y base de datos que se realiza periódicamente?
Criterio de puntuación: *0 – No existe política de respaldo. 5 – Existe pero no es adecuada. 10 – Existe y es adecuada.*

A.1.3 ¿Se cuenta con un plan de contingencia para reestablecer el Sitio Web en caso de un ataque o falla?
Criterio de puntuación: *0 – No existe plan de contingencia. 5 – Existe pero no es adecuada. 10 – Existe y es adecuada.*

B Estándares sobre estructura tecnológica

B-1 Configuración de Seguridad

B.2 Configuración de Acceso

B.1 Configuración de Seguridad

B.1.1 ¿Se evita que sea visto, el nombre de los directorios y archivos?
Criterio de puntuación: *0 – Se puede ver el nombre del directorio. 5- Se puede ver el directorio en algunos directorios y en otros no. 10- No se puede ver. Algún mensaje de error de acceso aparece.*

B.1.2 ¿Se tiene los permisos de lectura, escritura y ejecución adecuados para los directorios 775 y archivos 664?
Criterio de puntuación: *0 – No se tienen los permisos de directorio y archivos adecuados. 5- No se tienen todos los permisos de los directorio y archivos. 10- Se tienen los permisos de directorio y archivos adecuados.*

B.1.3 Cuando se accede a una página que no existe, ¿se ofrece un mensaje que le permita encontrarla en su nueva ubicación?
Criterio de puntuación: *0 – No se ofrece ningún mensaje más allá de la página estándar del servidor. 5 – Se ofrece una página 404 que explica la causa del error en idioma castellano. 10 – Se ofrece una página 404 que explica la causa del error e incluye un buscador para buscar la página que no se ha encontrado.*

B.1.4 Se han realizado las 10 configuraciones de seguridad mínimas a nivel de servidor web y lenguaje de programación definidas por ITIGES:
Criterio de puntuación: *0 – No han realizado. 5 –Se han realizado pero no en su totalidad – 10 Se han realizado todas.*

B.2 Configuración de Acceso

B.2.1 ¿Las páginas son visibles fácilmente por usuarios con conexiones lentas?
Criterio de puntuación: *de 0 -10 =10 - de 10 s en adelante = 0*

B.2.2 ¿El Sitio cuenta con un archivo de texto Robots.txt para los directorios que no se desea indexar?
Criterio de puntuación: *0 – No existe. 5- Existe pero su contenido no es adecuado 10 – Existe.*

B.2.3 ¿El Sitio cuenta con un archivo de texto sitemap.xml que ofrece los enlaces del sitio web, para que sea indexado en buscadores?
Criterio de puntuación: *0 – No existe. 5- Existe pero su contenido no es adecuado 10 – Existe.*

B.2.4 El sitio se encuentra indexado en las herramientas para Webmasters de Google http://www.google.com/webmasters/
Criterio de puntuación: *0- El Sitio Web no esta indexado en la herramienta de google 10- El Sitio Web está indexado en las herramientas webmaster de google.*

B.2.5 El Sitio Web está vinculado a una cuenta de google analytics y genera estadísticas de navegación:
Criterio de puntuación: *0 – No tiene. 5 – Existen pero no está generando estadísticas – 10 Existe y genera estadísticas.*

B.2.6 El Sitio Web está protegido a través de archivo .htaccess, para filtrado de URL:
Criterio de puntuación: *0 – No tiene archivo .htacccess . 5 – Existen pero no filtra las URL 10 – Existe y filtra las URL.*

B.2.7 ¿El Sitio ofrece un contenido adecuado para el tag HTML META NAME="description"?
Criterio de puntuación: *0 – No existe. 5 – Existe pero no es adecuado. 10 – Existe y es adecuado*

B.2.8 El Sitio ofrece un contenido adecuado para el tag HTML META NAME="keywords"?
Criterio de puntuación: *0 – No existe. 5 – Existe pero no es adecuado. 10 – Existe y es adecuado*

B.2.9 ¿Tiene definido el texto que aparece en el tag HTML < title > para indicar el Nombre del Sitio o de la Institución?
Criterio de puntuación: 0 – No aparece el nombre del sitio o institución en la barra de título. 5 – Aparece en algunas páginas. 10 – Aparece en todas las páginas.

B.2.10 El Sitio Web es acezado a través de URL Amigables o fácil interpretación:
Criterio de puntuación: *0 – No tiene URL Amigable. 5 – Existen pero no son las adecuadas 10 – Existe y son los adecuados.*

B.2.11 Consistencia de todos los enlaces
Criterio de puntuación: *(Número de enlaces rotos / Número de enlaces totales) * 10*

C Estándares sobre Diseño y Comunicación

C.1 Diseño Estructural

C.1 Diseño Estructural

C.1.1 Estructura de navegación del sitio en tres clics
Criterio de puntuación: *0 – La estructura tiene más de cuatro niveles jerárquicos de navegación 10 – La estructura tiene menos de cuatro niveles jerárquicos de navegación.*

C.1.2 Estructura de navegación del sitio coherente
Criterio de puntuación: *Criterio a considerar: Las agrupaciones y subagrupaciones son lógicas y agrupan elementos similares (por ejemplo, no agrupan un documento legal junto a una información sobre el organigrama) 0 – La estructura de navegación es profundamente desorganizada e incoherente 5 – La estructura de navegación es coherente en unas agrupaciones, pero puede mejorarse en otras. 10 – La estructura de navegación es coherente en todas las agrupaciones.*

C.1.3 Se sigue la estructura de navegación estándar para los primero 2 niveles de navegación
Criterio de puntuación: *0- No se sigue la estructura de navegación estándar 5- Se sigue pero no en su totalidad 10- Se sigue en su totalidad*

C.1.4 El Sitio Web mantiene la distribución espacial estándar de los elementos en cuanto a su ubicación y distribución de los elementos:
Criterio de puntuación: *0 – No tiene. 5 – Existen pero no es la adecuada – 10 Existe y es la adecuada.*

C.1.5 Las páginas del sitio incluyen el logo y la pertenencia al gobierno. ***Criterio de puntuación:*** *0 – Ninguna 3 – Sólo la portada y no muestra el logo de forma visible y permanente en todas las páginas del sitio web. 6- La portada, algunas páginas. 10 – Todas las páginas sin excepción y mantiene la integridad del logo.*

C.1.6 El Sitio Web mantiene la barra de proyectos estratégicos del Gobierno. ***Criterio de puntuación:*** *0 – No tiene. 5 – Existen pero no es la adecuada al no estar automatizada – 10 Existe y es la adecuada.*

C.1.7 El URL corresponde con el nombre de la institución o la función.
Criterio de puntuación: *10 – corresponde. 0 – No corresponde.*

C.1.8 ¿Los íconos utilizados en el sitio web son representativos de la función o acción que realizan?
Criterio de puntuación: *0 – No son representativos 5- Algunos iconos son representativos 10- Todos los iconos son representativos*

D-Estándares sobre Accesibilidad

D.1 Diseño Accesible

D.1 Diseño Accesible

D.1.1 ¿La información transmitida a través de los colores también está disponible sin color?
Criterio de puntuación: *0 – No se distinguen las informaciones principales con los filtros de color. 5 – Algunas informaciones no se distinguen o tienen poco contraste con estos filtros. 10 – Todas las informaciones se distinguen perfectamente con los filtros de color.*

D.1.2 Se distingue en el sitio entre los enlaces visitados y no visitados.
Criterio de puntuación: *0 – No se distingue. 10 – Se distingue*

D.1.3 ¿El tamaño de la letra de los textos es ajustable o modificable por el usuario usando las herramientas del programa visualizador?
Criterio de puntuación: *0 – No es modificable 10 –Si lo es*

D.1.4 ¿Se proporciona un texto equivalente para todo elemento no textual, tales como imágenes y animaciones, para explicar su contenido?
Criterio de puntuación: *0 – De ninguna imagen se proporciona un texto alternativo. 2- Pocas imágenes tienen un texto alternativo. 4- Algunas imágenes informativas proporcionan un texto alternativo pero no todas. 9- Todas las imágenes informativas proporcionan un texto alternativo, pero no se proporciona texto "" para las imágenes decorativas. 10- Todas las imágenes proporcionan un texto alternativo, incluso las decorativas.*

D.1.5 El Sitio Web es compatible e interpretado a través de dispositivos Móviles:
Criterio de puntuación: *0 – No compactible. 5 – No es compactible por al menos 3 tipos de dispositivos – 10 Es compactible y es la adecuada*

D.1.6 El Sitio Web es compatible por al menos 4 Navegadores incluyendo Internet Explorer Versión 7:

Criterio de puntuación: *0 – No compactible. 5 – No es compactible por al menos 3 navegadores – 10 Es compactible y es la adecuada*

D.1.7 Se Utiliza hojas de estilo o lenguaje de marcado para reemplazar los elementos de accesibilidad baja
Criterio de puntuación: *0 – No se utiliza 10 –Si se utiliza*

D.1.8 Se evita el llamado de ventanas emergentes; de no ser posible eliminar se anuncia previamente su aparición
Criterio de puntuación: *0 – No se evita. 5 – Se ocupa solo para imágenes o elementos multimedia – 10 Se evitan o estos son accesibles.*

D.1.9 Se evita el movimiento de las páginas; o de no ser posible eliminarlo se anuncia debidamente su presencia
Criterio de puntuación: *0 – No se evita. – 10 Se evitan o se le brinda controles del movimiento de forma accesible al usuario.*

E- Estándares sobre Contenido

E.1 Contenido estático

E.2 Contenido dinámico

E Estándares sobre Contenido

E.1 Contenido estático

E.1.1 El sitio incluye la filosofía de la organización: Misión, visión y valores.
Criterio de puntuación: *0 – No existe 5 – Existe y es incompleta. 10 – Existe y es completa*

E.1.2 Hay cartas de derechos.
Criterio de puntuación: *0 - No hay cartas de Derechos. 5 – Las hay, pero no están suficientemente destacadas. 10- Las hay y están suficientemente destacadas.*

E.1.3 Hay documento de política de seguridad y de política de privacidad.
Criterio de puntuación: *0 – No existe documento de política. 10 – Existe.*

E.1.4 Las páginas incluyen al pie de la página el nombre de la institución y los contactos virtuales y físicos.
Criterio de puntuación: *0 – Ninguna 3 – Sólo la portada. 6- La portada y algunas páginas. 10 – Todas las páginas sin excepción.*

E.1.5 Existen accesos a herramientas de participación ciudadana accesibles desde la portada del Sitio Web:
Criterio de puntuación: *0 – No existe ninguno. 5 – Existen al menos dos de los siguientes: Formulario de contacto, Facebook, Twitter, Google +, Foros 10 – Existen más de dos.*

E.1.6 El Sitio Web contiene en la sección de ubicación la información de sus direcciones físicas, mapas y teléfonos de contactos de sus instalaciones y sucursales:
Criterio de puntuación: *0 – No tiene. 5 – Existen pero no es el adecuado – 10 Existe y es la adecuada.*

E.2 Contenido dinámico

E.2.1 ¿Las estadísticas, cumplimiento de metas, resultados de encuestas, tablas, cuadros comparativos son presentados en más de una alternativa? Excel o CSV como básico
Criterio de puntuación: *0 – No hay estadísticas, cumplimiento de metas, resultados de encuestas, cuadros comparativos o sólo se presentan en un formato que no es CSV, normalmente, en formato de imagen. 5 – Cada estadística, cumplimiento de metas, resultados de encuestas, cuadros comparativos se presentan en varios formatos, pero CSV no es uno de ellos. 10 – Cada estadísticas, cumplimiento de metas, resultados de encuestas, cuadros comparativos se presentan en varios formatos, siendo para cada uno CSV uno de ellos.*

E.2.2 Existe una sección de descarga en donde los archivos (documentos, comprimidos, imágenes, audios y videos) deben de estar disponibles para poder ser descargados
Criterio de puntuación: *0 – Los archivos publicados no pueden ser descargar. 5 – Algunos archivos publicados no pueden ser descargados. 10 – Todos los archivos publicados son descargados.*

E.2.3 En la portada se puede acceder a las secciones principales, servicios, avisos, elementos multimedia, proyectos y noticias.
Criterio de puntuación: *0 – No se puede acceder a ninguno de estos elementos 5 – Se puede acceder al menos a tres elementos 10 - Se puede acceder a más de tres elementos.*

E.2.4 Las páginas de noticias, avisos y servicios tienen fecha de actualización.
Criterio de puntuación: *0 – Ninguna página tiene fecha de actualización. 3 – Unas pocas páginas la tienen. 7- La mayoría de páginas tienen fecha de actualización. 10 – Todas las páginas tienen fecha de actualización.*

E.2.5 El Sitio Web maneja una sección de publicaciones y descarga de documentos de interés de la ciudadanía:
Criterio de puntuación*: 0 – No tiene. 5 – Existen pero con muy poca información o en desroden – 10 Existe y es la adecuada.*

E.2.6 El sitio ofrece noticias o notas de prensa.
Criterio de puntuación: *0 – No hay sección de noticias. 5 - Sección de noticias publicadas con periodicidad baja. 10 – Sección de noticias.*

E.2.7 El sitio ofrece agenda de eventos.
Criterio de puntuación: *0 – No hay sección de eventos. 5 - Sección de eventos publicadas con periodicidad baja . 10 – Sección de eventos.actualizada*

E.2.8 Hay una guía de servicios, donde se describe los servicios que da la institución junto con los requisitos, precios, formularios correspondientes, horarios de atención y correo electrónico para consultas.
Criterio de puntuación: *0 – No hay guía de servicios. 5 – Existe una guía de servicios con su descripción, pero no está completa. 10 – Hay una guía de servicios completa.*

E.2.9 Existe una lista de servicios más demandados que presta la institución accesible a través de la portada (redirección o enlace a la descripción completa del servicio):
Criterio de puntuación: *0 – No existe. 5 – Presenta los servicios pero no están enlazados, 10 – Presenta los servicios y están debidamente enlazados o re-direccionados.*

E.2.10 El Sitio Web publica información de proyectos de interés ciudadano
Criterio de puntuación: *0 – No tiene. 5 – Proyectos publicados sin datos completos – 10 Descripción del proyecto, fuente de financiamiento, fecha de inicio, fecha de finalización.*

E.2.11 Hay una página de preguntas frecuentes.
Criterio de puntuación: *0 - No existe una página de preguntas frecuentes 10 –Existe una página de preguntas frecuentes.*

F- Estándares sobre Uso y Funcionalidad

F.1 Funcionalidades

F.2 Uso de Sitio Web

F Estándares sobre Uso y Funcionalidad

F.1 Funcionalidades

F.1.1 Traducción al inglés de las páginas.
Criterio de puntuación: *0 – No lo tiene. 10 – Ocupa como mínimo Google Translator*

F.1.2 Existe un Mapa del sitio.
Criterio de puntuación: *0 – No existe. 5 – Existe, pero no es claro o no tiene una presentación visual correcta 10- Existe, es claro y tiene una presentación visual.*

F.1.3 Hay un rastro de navegación que indica el camino que se ha llegado desde la portada a la página que se está visualizando.
Criterio de puntuación: *0 – No hay rastro de navegación. 10 – Sí que lo hay.*

F.1.4 Existe un mecanismo de búsqueda que sea accesible en todas las páginas del Sitio Web.
Criterio de puntuación: *0 – No existe. 5 – Existe pero no da buenos resultados, no muestra los resultados de forma correcta o no se encuentra en todas las páginas. 10 – Existe, da buenos resultados, que muestra de forma correcta y se encuentra en todas las páginas.*

F.1.5 Los formularios están validados con Javascript y una vez se produce un error se vuelve a la misma página con indicaciones sobre qué hay que corregir.
Criterio de puntuación: *0 – No hay formularios online, éstos no están validados o bien están validados sin Javascript (por ejemplo, validación del lado del servidor). 5- Los formularios están validados con Javascript pero no se vuelve a la misma página o no se indican las correcciones. 10- Los formularios están validados con Javascript, se dan indicaciones y se indica qué hay que corregir.*

F.1.6 Usa elementos destacados para indicar los campos obligatorios dentro de un formulario y muestra un mensaje al enviar el formulario.

Criterio de puntuación: *0 – No hay formularios online o los campos obligatorios no están indicados. 5- Los campos obligatorios están indicados pero no existe la frase que lo explica, del estilo de "Los campos con asterisco son obligatorios" o no muestra mensaje al enviar . 10 – Están indicados los campos y existe una frase indicándolo y envía mensaje al enviar el formulario.*

F.1.7 El Sitio Web contiene Fuentes de Indexación RSS en sus noticias, servicios, publicaciones, Avisos y proyectos:
Criterio de puntuación: *0 – No tiene. 5 – Existen pero no es el adecuado – 10 Existe y es la adecuada.*

F.2 Uso de Sitio Web

F.2.1 ¿Los documentos oficiales mostrados en formato PDF, imagen o flashpaper son mostrados al mismo tiempo en su fuente original o versión accesible (Word, Excel, Powerpoint, etc)

Criterio de puntuación: *0 – Los documentos son mostrados solamente en formatos no accesibles. 5 – Algunos documentos son mostrados en formatos no accesibles. 10 – Todos los documentos son mostrados en formato accesible.*

F.2.2 Los archivos (documentos, audios y videos) son publicados con licencias Creative Commons a menos que existan impedimentos legales.

Criterio de puntuación: *0 – Los archivos son publicados con derechos reservados. 5 – Algunos archivos son publicados con derechos reservados. 10 – Todos los archivos son publicados con creative commons.*

F.2.3 La información del Sitio Web contiene los derechos de información bajo licencia Creative Commons.

Criterio de puntuación: *0 – El Sitio web tiene derechos reservados. 10 – El Sitio Web esta licenciado bajo creative commons.*

F.2.4 Existen opciones para compartir contenido con las redes sociales.

Criterio de puntuación: *0 – No existe. 5 – Existe, pero no es claro o no vincula al menos con 3 redes sociales 10- Existe, es claro y vincula con más de 3 redes sociales.*

F.2.5 Existen opciones para seguir las redes sociales institucionales.

Criterio de puntuación: *0 – No existe. 5 – Existe, pero no es claro o no vincula al menos con 3 redes sociales 10- Existe, es claro y vincula con más de 3 redes sociales.*

Dirección de Medios Digitales y Redes Sociales
Secretaría de Gobernabilidad y Comunicaciones
Dirección de Innovación Tecnológica e Informática
del Gobierno de El Salvador.
Casa Presidencial de la República de El Salvador,
Alameda Dr. Manuel Enrique Araujo, 5500
San Salvador, El Salvador.

10 RECOMENDACIONES DE SEGURIDAD

1.- ACTIVAR EL URL AMIGABLES

La activación de las URL Amigables consiste básicamente en tres pasos:

1. Realizar las configuraciones de apache
2. Subir un archivo .htaccess al raíz de la carpeta de publicación del Sitio Web
3. Activar las correspondientes en las opciones de lectura de Wordpres!

Configuraciones de apache

- Ingrese a la configuración de apache, guarde una copia antes de realizar esta acción y edite el archivo de configuración "httpd.conf"
- busca la linea donde dice:
  #LoadModule rewrite_module modules/mod_rewrite.so

  Quilatarle el "#"
  [se cambia ha esto:]
  LoadModule rewrite_module modules/mod_rewrite.so
- El servidor debe tener el mod_rewrite habilitado.
- El servidor debe permitir manejar el archivo .htaccess.
- Reinicie el servidor apache

Sin URLs amigables: http://www.presidencia.gob.sv/index.php?p=24

Con URLs amigables: http://www.presidencia.gob.sv/presidente-sanchez-ceren-se-reune-con-equipo-de-funcionarios-para-dar-seguimiento-al-tema-de-seguridad/

Se recomienda revisar posteriormente los enlaces del Sitio web pues muchos de ellos pudieron haber cambiado con este proceso

2.- UTILIZAR PERMISOS A NIVEL DE .HTACCESS

Cree un archivo .htaccess que permita configurar permisos y filtre las url de su sitio web, como el que se muestra a continuación:

```
# Protege wpconfig.php
<files wp-config.php>
order allow,deny
deny from all
</files>
# Protege los Plugin
<Files ~ "\.(js|css)$">
  order allow,deny
  allow from all
</Files>
# Protege el archive htaccess
<Files .htaccess>
order allow,deny
deny from all
</Files>
# Evite la Navegación de directorios
Options All -Indexes
 # desactiva la firma del servidor
ServerSignature Off
 # limita la carga de archivos a 10mb o lo que considere uso normal en su Sitio Web
LimitRequestBody 10240000
 #documentos personalizados de error para redireccionar a páginas de error(lo cambias por los tuyos)
ErrorDocument 404 /notfound.html
ErrorDocument 403 /forbidden.html
ErrorDocument 500 /error.html
 # establece la url canonica (amigable)
```

```
RewriteEngine On

RewriteCond %{HTTP_HOST} ^tudominio\.com$ [NC]

RewriteRule ^(.*)$ http://www.tudominio.com/$1 [R=301,L]

 # protege de comentarios SPAM

RewriteEngine On

RewriteCond %{REQUEST_METHOD} POST

RewriteCond %{REQUEST_URI} .wp-comments-post\.php*

RewriteCond %{HTTP_REFERER} !.*tudominio.com.* [OR]

RewriteCond %{HTTP_USER_AGENT} ^$

RewriteRule (.*) ^http://%{REMOTE_ADDR}/$ [R=301,L]

RewriteRule ^post/([0-9]+)?/?([0-9]+)?/?$ /index.php?p=$1&page=$2 [QSA]

#Protege las URL Filtrandolas de Ataques

# Block out any script trying to set a mosConfig value through the URL

RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]

# Block out any script trying to base64_encode crap to send via URL

RewriteCond %{QUERY_STRING} base64_encode.*\(.*\) [OR]

# Block out any script that includes a <script> tag in URL

RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]

# Block out any script trying to set a PHP GLOBALS variable via URL

RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]

# Block out any script trying to modify a _REQUEST variable via URL

RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})

# Send all blocked request to homepage with 403 Forbidden error!

RewriteRule ^(.*)$ index.php [F,L]

#Desactiva el TRACE de HTTP y TRACK

RewriteEngine on

RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)

RewriteRule .* - [F]
```

3.- REVISION DE ERRORES

- Regularmente revise los registros de log a nivel de servidor Web Apache, MySQL y PHP para identificar posibles ataques o intentos de ingresar al Sitio Web
- Desactive la impresión en pantalla de los errores de PHP y redirija las páginas de error en el apache para que no se muestren estos errores.

4.- HTTP SERVER (APACHE, ETC.)

- PHP, MySQL y muchos otros componentes base fueron originalmente diseñados para, y generalmente funcionan mejor en, servidores Apache. Evite usar otros servidores.
- Regularmente revise los registros de acceso en busca de actividad sospechosa. No confíe en sumarios y gráficas. Revise los "raw logs" (registros en crudo) para detalles más reales.
-
- Configure los filtros de Apache mod_security y mod_rewrite para que bloqueen ataques PHP.

5.- SEGURIDAD EN MYSQL

- Asegúrese de que la cuenta MySQL del Usuario de conexión no sea el root y este tenga los permisos adecuados. Este consciente de que la instalación inicial de MySQL es insegura. Una cuidadosa configuración manual es requerida luego de la instalación. De ser posible ocupe Socket de conexión a MySQL
- En un servidor compartido, si usted puede ver los nombres de las bases de datos de otros usuarios, entonces puede estar bastante seguro de que ellos ven las suyas. Si ellos pueden ver las bases de datos que usted posea, ellos están innecesariamente un paso más cerca de entrar. Un buen ISP limitara estrictamente el acceso de cada usuario a sus propias bases de datos.

6.- SEGURIDAD CON PHP

- Antes que nada PHP 4 ya no es mantenido activamente, actualice su código PHP a PHP 5, y se recomienda utilizar la versión 5.2.9.
- Aplique todos los parches necesarios para PHP y para aplicaciones basadas en PHP.
- Se recomienda un frecuente escaneo web en ámbitos donde un gran número de aplicaciones PHP están en uso.
- Utilice herramientas como Paros Proxy para realizar pruebas automáticas de SQL Injection en contra de sus aplicaciones PHP.

- Siga el principio de "Least Privilege" (El menor privilegio) para correr PHP usando herramientas como PHPsuExec, php_suexec o suPHP.

7.- CONFIGURACION DE ARCHIVO PHP.INI

- Estudie la lista oficial de directivas php.ini en www.php.net.

- Configure register_globals OFF. Esta directiva determina si registrar o no las variables EGPCS (Environment, GET, POST, Cookie, Server) como variables globales.

- Use disable_functions para desactivar peligrosas funciones PHP que no son necesarias para su sitio.

- Desactive allow_url_fopen. Esta opción activa las URL-aware fopen wrappers que permite el acceso a los objetos URL como archivos. Los wrappers (envolturas) son proveídos para el acceso de archivos remotos usando el ftp o el protocolo http, algunas extensiones como zlib son capaces de registrar wrappers adicionales. Nota: Esto solo puede ser configurado en php.ini por motivos de seguridad.

- Ajuste la directiva magic_gpc_quotes como sea necesario para su sitio. Debería estar en off para usar software bien escrito, y para los pobremente escritos scripts PHP 3 y PHP 4 . magic_gpc_quotes configura el estado magic_quotes state para operaciones GPC (Get/Post/Cookie). Cuando magic_quotes esta on, todas las ' (single-quote/comillas-simples), " (double quote/comillas dobles), \ (backslash-barra invertida) y NUL's son evitadas con una barra invertida \ automáticamente.

- Modo Seguro: safe_mode (debería estar activado y configurado correctamente)

- open_basedir (debería estar activado y configurado correctamente). Limite los archivos que pueden ser abiertos por PHP al árbol de directorios especificado, incluyendo el archivo mismo. Esta directiva no es afectada si el Safe Mode esta On u Off. La restricción especificada con open_basedir es en realidad un prefijo, no un nombre de directorio. Esto significa que "open_basedir = /dir/incl" también permite el acceso "/dir/include" y "/dir/incls" si es que existen. Cuando quiere restringir el acceso solamente al directorio especificado, cierre con una barra /.

- error_reporting = E_COMPILE_ERROR|E_ERROR|E_CORE_ERROR muestra solo errores.

- display_errors = Off determina si los errores se visualizan en pantalla como parte de la salida en HTML o no. Como queda dicho, es desaconsejado mostrar errores en pantalla en páginas visibles al público.

Aquí hay directivas de ejemplo para las sugerencias anteriores:

register_globals = 0

disable_functions = show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open

allow_url_fopen = 0

magic_gpc_quotes = 0

safe_mode = 1

open_basedir = /dir/incl/

8.- PROTEGER EL ADMINISTRADOR DE WORDPRESS

El tema de la seguridad en los Sitios Web es algo muy importante. Debido a que la ruta de acceso a la administración de Wordpress es siempre la misma: (http://www.tusitio.com/wp-admin), cualquiera pudiera intentar entrar, hacer de las suyas y más si aun tienes el usuario "admin" o "root" activo y como administrador.

Para poner una barrera de seguridad adicional a nuestro sitio, existen algunos plug-in muy efectivo y sencillo de utilizar que modifica la ruta de acceso a la administración: Custom WP-Admin. Principalmente se trata de cambiar la url de administración para personalizar nuestra ruta del administrador.

Pasos a seguir:

Primero debéis descargar el plug-in https://wordpress.org/plugins/hc-custom-wp-admin-url/

Después hay que instalarlo desde los plugin una vez instalado, entramos en el Gestor de plug-ins y lo activamos.

Luego ingresamos a las opciones permanentes de enlaces en la administración y buscamos el **WP-Admin slug**. Se debe de ingresar la contraseña que cambiara la

Si nuestra clave es por ejemplo: **adminprotegido**

http://www.misitio.gob.sv/**adminprotegido**/

9.- ACTUALIZACIONES DE SITIO WEB

- Siempre actualice a la última versión estable del Core de Wordpress. Este proceso es sumamente sencillo ya que Wordpress avisa cuando hay nuevas versiones y solamente se deben de dar clic en actualizar, es recomendable que si se hacen modificaciones en las funciones de wordpress tenga en cuenta que estas serán afectadas con la actualización y deberá estar pendientes para volver a generarlas.
- Revisar los permisos de los directorios de Wordpress después de instalarlo los directorios que tenga una máscara de permisos mayor de 755 pueden comprometer la seguridad.

- Revisar los permisos de los ficheros recomendado usar una máscara de permisos de 644 o más restrictiva.

10.- ACTUALIZACIONES DE EXTENSIONES

- Pruebe las extensiones antes de actualizarlas o instalarlas de forma local o en servidor de desarrollo.
- Descargue extensiones solo de sitios de confianza. La definición oficial de "sitio de confianza" es aquel sitio en el que USTED confía.

- Remueva cualquier extensión no usada, y revise doblemente que los directorios y archivos relacionados hayan sido borrados.