Termos de uso hospedagem de dados em Wordpress

Curitiba, 15/01/2019 – CNPJ 20.962.496/0001-91 – IDC 2112
REG: 05/06/2014 Registro Contrato e termos de uso de dados e exclusividade.

O Provedor HOSTCURITIBA protocolou nestes Termos de Uso as condições para utilização deste site de forma a estabelecer as obrigações e responsabilidades de seus usuários.
Ao usar os serviços de hospedagem de scripts em wordpress o usuário concorda e aceita integralmente as condições estabelecidas nos Termos de Uso abaixo descritas.

O usuário não poderá praticar as seguintes ações com relação ao site hospedado se a estrutura wordpress não atuar em conformidade com as proteções e métricas de segurança padrões de modo a contrariar a ordem segura ou atentar contra a moral de acessos e dados de um servidor.

- Utilizar o site e/ou qualquer conteúdo dele constante, no todo ou em parte, com propósito diverso daquele a que este se destina e de forma diversa da prevista nestes Termos de Uso;
- Apagar, corromper, editar ou de qualquer forma modificar, sob qualquer meio ou forma, no todo ou em parte, o site e/ou qualquer conteúdo dele constante;
- Fazer publicidade ou marketing associando sua imagem pessoal à ou a qualquer empresa sob controle direto ou indireto do Conglomerado Econômico-Financeiro;
- Praticar quaisquer atos em relação ao site, direta ou indiretamente, no todo ou em parte, que possam causar prejuízo a ou a qualquer usuário em navegação;
- Usar qualquer nome empresarial, marca, nome de domínio, slogan, expressão de propaganda ou qualquer sinal distintivo ou bem de propriedade intelectual de titularidade ou de qualquer empresa sob o controle direto ou indireto do Conglomerado
- usar, sob qualquer meio ou forma, o site, sua identidade visual (especialmente o projeto de arte gráfico-visual de quaisquer de suas páginas) ou qualquer conteúdo ou obra intelectual nele inserido de titularidade de outros websites tais como clones de informações e imagens;
- Praticar falsidade de informações e falsidade ideológica;
- Praticar qualquer ato contrário à boa-fé e aos usos e costumes, que possam ofender qualquer direito de terceiros e que esteja em desacordo com a etiqueta da Internet comumente aceita;
- Cometer fraude;
- Usar de programações ultrapassadas e vulneráveis como bibliotecas javas desatualizadas
- Cadastrar-se em sites de segurança, notificando em seu e-mail sobre plugins vulneráveis.
- Usar de temas baixados pela internet sem qualquer ação de verificação de vulnerabilidades.
- Usar de temas Nulled hackeados e estes com uso de BASE64 com chaves ofuscadas.
- Desenvolver scripts que não são suportadas com as tecnologias do servidor atual.
- Injetar qualquer Scripts para monitorar, tentar ou forçar ataques ao servidor de formas e meios sem o conhecimento da ferramenta e suas causas direcionadas ao servidor ou dados.
- Manter Wordpress com temas, plugins e informações desnecessárias na raiz do seu ftp servidor comprometendo os dados do servidor e informações de coletadas das tecnologias.
- Não atualizar ou abandonar o wordpress com falhas, logs e ações que sobrecarreguem o servidor pode ser suspenso ou removidos.
- Não aplicar endurecimento e proteção para acessos, pastas ou manter wordpress padrão.
- Não instalar ou configurar o wordpress para somente o uso de SSL em todo o ambiente
- Configurar e-mail do domínio com senhas no wordpress, pode ter a conta suspensa imediato.
- Propagar, distribuir ou transmitir códigos destrutivos, que tenham ou não causado danos reais;
- Utilizar robôs, "spiders" ou qualquer outro dispositivo ou sistema, automático ou manual, para monitorar ou copiar qualquer conteúdo;
- Forçar scripts sem autorização, por meio de práticas de "hacking", "password mining" ou qualquer outro meio fraudulento ou que represente violação a direito de terceiros;
- Provocar a vulnerabilidade dos sistemas em Tecnologia da Informação que, direta ou indiretamente, fazem parte da infraestrutura que suportam o website, para obter e utilizar quaisquer informações neles constantes;
- Ajudar qualquer terceiro a realizar qualquer uma das ações vedadas por este Termos de Uso

Em nenhuma hipótese, a HOSTCURITIBA será responsável:

- Por qualquer ato ou omissão realizado e/ou dano causado pelo usuário no âmbito do site;

- Pelo uso indevido por qualquer usuário ou terceiros do site, no todo ou em parte, por qualquer meio ou forma, inclusive por meio de sua reprodução e/ou divulgação, especialmente em sites da Internet;
- Pela suspensão, remoção ou interrupção do site, falta de manutenção ou apoio não acordado.

A tolerância do Provedor HOSTCURITIBA quanto ao eventual descumprimento de quaisquer das disposições destes Termos de Uso e/ou demais políticas do site por qualquer usuário não constituirá renúncia ao direito de exigir o cumprimento da obrigação, nem perdão, nem alteração do que consta aqui previsto.
A HOSTCURITIBA poderá, a qualquer tempo, a seu exclusivo critério e sem necessidade de qualquer aviso prévio ou posterior a qualquer usuário ou terceiros, tirar o site do ar e alterar e/ou atualizar no todo ou em parte estes Termos de Uso. Qualquer alteração e/ou atualização destes Termos de Uso passará a vigorar a partir da data de sua publicação no site e deverá ser integralmente observada pelos usuários.

Sem prejuízo de outras medidas, o Provedor HOSTCURITIBA poderá, por si ou por terceiros, a qualquer tempo, a seu exclusivo critério, sem necessidade de qualquer aviso ou notificação prévia ou posterior a qualquer usuário sob qualquer meio ou forma, sem prejuízo de iniciar as medidas legais cabíveis, suspender o acesso ao site de qualquer usuário, a qualquer tempo, caso o usuário descumpra qualquer disposição destes Termos de Uso e demais políticas do site ou a lei.

Política de Privacidade
Esta Política de Privacidade foi criada para demonstrar o compromisso da Provedora HOSTCURITIBA com a segurança e a privacidade das informações recebidas por seus usuários, bem como para esclarecer como essas informações são coletadas e tratadas.

Ao fornecer informações pessoais ou navegar neste site, o usuário estará automaticamente concordando com as regras aqui estabelecidas e concorda com as aplicações e ações exigidas;

Não poderá ser exigida em seu website informações confidenciais, como número de cartão de créditos e para os demais dados pessoais dos usuários serão igualmente mantidos em sigilo e jamais divulgados sem autorização, salvo quando exigidos por Lei ou determinação judicial.

Todas as informações são coletadas mediante conhecimento e consentimento dos usuários, e são utilizadas para atender ao propósito para o qual as informações foram fornecidas e divulgar os produtos e serviços que possam ser do interesse dos usuários:

- Os usuários saberão quais informações suas coletaremos, ficando a opção de fornecer ou não essas informações sob a responsabilidade do usuário, o qual também terá ciência das consequências de sua decisão;

- Informações pessoais dos usuários não poderão ser compartilhadas com empresas contratadas para prestação de serviços de comunicação, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados podendo as mesmas com vendas de informações

- A menos que tenhamos determinação legal ou judicial, suas informações nunca serão transferidas a terceiros ou usadas para finalidades diferentes daquelas para as quais foram coletadas.

Por fim, o presente site deve verificar antes de fornecer links (conexões) para outros sites externos. A HOSTCURITIBA não se responsabiliza pelas políticas de privacidade nem pelo conteúdo de tais sites. Recomendamos que você leia tais políticas antes de iniciar a produção de seu wordpress.

WordPress é seguro?

WordPress sempre será a plataforma mais amada por todos e assim como tudo que é on-line precisa de atenção. Acredito que não podemos afirmar que wp é totalmente inseguro sabendo que os critérios básicos para entender a segurança de qualquer estrutura são sempre:

1) Atualizar o núcleo automaticamente conforme ele é iniciado
2) Gerar backups frequentes para recuperação ou retrocesso
3) Atualize plugins e use principalmente addon com fontes seguras e suportadas
4) Use os plugins de segurança mais votados e de atualização máxima possível

5) Não mantenha addons desnecessários e arquivos raiz como: readme.txt
6) Use técnicas para esconder o máximo que puder: versões do núcleo, versões do seu servidor Apache, e bloquear entradas como: pastas e admin
7) funções htaccess com limitações locais e bloqueios de menus wordpress
8) Rever log completo todos os dias, e buscar entradas suspeitas via addon
9) Solicitar hospedagem com segurança e as principais ferramentas de ataque.
10) Pergunte se o seu servidor possui ferramentas de níveis como: Pyxsoft Anti Malware, Imunify 360, MailScanner, ConfigServer Security & Firewall, Edge Protection para DDoS, Permite criptografar SSL para seu domínio ou nome de host, ferramenta de painel Hosting para limpeza e varredura entre outros.

11) Conecte-se em redes seguras conhecidas e não salve senhas em ambientes
12) Remova temas desnecessários de pastas de temas
13) Acesse o relatório e os plugins de backup

Olhe atentamente para cada ação que os alertas wordpress e backup garantido ainda não é totalmente seguro, então desistir wordpress parece ser ideias inseguras.

A rede está a salvo do wordpress, o que devemos fazer é provar que existe uma maneira de fazer a coisa certa.

Uma data center que mantém o DDoS nas fronteiras, um provedor de hospedagem com várias ferramentas de proteção unindo-se ao seu compromisso de vigiar e endurecer o seu wordpress e a atenção diária, torna-o único em não ataques e tem monitoramento para ele.

Instalar addons adicionais para a segurança do wordpress.
1. Proteção Wordfence = Firewall para todos
2. Disable-xml-rpc = Blocos injeção xmlrpc
3. Exploit-scanner = Frequent Scan
4. Heartbeat-control = Ajuda em recursos .ajax.php
5. Renomear-wp-login = Alterar o link de login
6. Wp-security-questions = Criar pergunta de segurança
7. wp-smushit = Compactar imagem

Verificar se o arquivo principal htaccess está munido de proteção
.htaccess com regras básicas de proteção ajuda como:
1. Bloquear pasta de Upload padrão
2. Edição de bloco de arquivos de administração
3. Instalação de plugins de bloco
4. Edição de temas de bloco
5. Remover menus desnecessários wp

Bloquear link do admin via htaccess:

```
$user_id = get_current_user_id();
if ($user_id == 1) { //em 10, adicione o ID do usuário que deseja remover os itens do menu
function remove_menus(){
remove_menu_page( 'themes.php' ); //Appearance – aparência (recomendo!)
remove_menu_page( 'plugins.php' ); //Plugins (recomendo!)
remove_menu_page( 'users.php' ); //Users – usuários
remove_menu_page( 'tools.php' ); //Tools – ferramentas (recomendo!)
remove_menu_page( 'options-general.php' ); //Settings – configurações
}
add_action( 'admin_menu', 'remove_menus' );
} else {}
```

Criar regras de compactação e segurança em seu servidor conforme a seguir:

```
# BEGIN LSCACHE
# END LSCACHE
# BEGIN NON_LSCACHE
# END NON_LSCACHE
# Configurações PHP.ini necessárias
<IfModule php5_module>
   php_flag asp_tags Off
   php_flag display_errors On
   php_value max_execution_time 300
   php_value max_input_time 300
   php_value max_input_vars 1000
   php_value memory_limit 512M
   php_value post_max_size 128M
   php_value session.gc_maxlifetime 1440
   php_value session.save_path "/var/cpanel/php/sessions/ea3"
   php_value upload_max_filesize 256M
   php_flag zlib.output_compression On
</IfModule>
# Configurações PHPini necessárias

# BEGIN W3TC Browser Cache
<IfModule mod_mime.c>
    AddType text/css .css
    AddType text/x-component .htc
    AddType application/x-javascript .js
    AddType application/javascript .js2
    AddType text/javascript .js3
    AddType text/x-js .js4
    AddType video/asf .asf .asx .wax .wmv .wmx
    AddType video/avi .avi
    AddType image/bmp .bmp
    AddType application/java .class
    AddType video/divx .divx
    AddType application/msword .doc .docx
    AddType application/vnd.ms-fontobject .eot
    AddType application/x-msdownload .exe
    AddType image/gif .gif
    AddType application/x-gzip .gz .gzip
    AddType image/x-icon .ico
    AddType image/jpeg .jpg .jpeg .jpe
    AddType image/webp .webp
    AddType application/json .json
    AddType application/vnd.ms-access .mdb
    AddType audio/midi .mid .midi
    AddType video/quicktime .mov .qt
    AddType audio/mpeg .mp3 .m4a
    AddType video/mp4 .mp4 .m4v
    AddType video/mpeg .mpeg .mpg .mpe
    AddType video/webm .webm
    AddType application/vnd.ms-project .mpp
    AddType application/x-font-otf .otf
    AddType application/vnd.ms-opentype ._otf
    AddType application/vnd.oasis.opendocument.database .odb
    AddType application/vnd.oasis.opendocument.chart .odc
    AddType application/vnd.oasis.opendocument.formula .odf
    AddType application/vnd.oasis.opendocument.graphics .odg
    AddType application/vnd.oasis.opendocument.presentation .odp
```

```
    AddType application/vnd.oasis.opendocument.spreadsheet .ods
    AddType application/vnd.oasis.opendocument.text .odt
    AddType audio/ogg .ogg
    AddType application/pdf .pdf
    AddType image/png .png
    AddType application/vnd.ms-powerpoint .pot .pps .ppt .pptx
    AddType audio/x-realaudio .ra .ram
    AddType image/svg+xml .svg .svgz
    AddType application/x-shockwave-flash .swf
    AddType application/x-tar .tar
    AddType image/tiff .tif .tiff
    AddType application/x-font-ttf .ttf .ttc
    AddType application/vnd.ms-opentype ._ttf
    AddType audio/wav .wav
    AddType audio/wma .wma
    AddType application/vnd.ms-write .wri
    AddType application/font-woff .woff
    AddType application/font-woff2 .woff2
    AddType application/vnd.ms-excel .xla .xls .xlsx .xlt .xlw
    AddType application/zip .zip
</IfModule>

<IfModule mod_expires.c>
    ExpiresActive On
    ExpiresByType text/css A31536000
    ExpiresByType text/x-component A31536000
    ExpiresByType application/x-javascript A31536000
    ExpiresByType application/javascript A31536000
    ExpiresByType text/javascript A31536000
    ExpiresByType text/x-js A31536000
    ExpiresByType video/asf A31536000
    ExpiresByType video/avi A31536000
    ExpiresByType image/bmp A31536000
    ExpiresByType application/java A31536000
    ExpiresByType video/divx A31536000
    ExpiresByType application/msword A31536000
    ExpiresByType application/vnd.ms-fontobject A31536000
    ExpiresByType application/x-msdownload A31536000
    ExpiresByType image/gif A31536000
    ExpiresByType application/x-gzip A31536000
    ExpiresByType image/x-icon A31536000
    ExpiresByType image/jpeg A31536000
    ExpiresByType image/webp A31536000
    ExpiresByType application/json A31536000
    ExpiresByType application/vnd.ms-access A31536000
    ExpiresByType audio/midi A31536000
    ExpiresByType video/quicktime A31536000
    ExpiresByType audio/mpeg A31536000
    ExpiresByType video/mp4 A31536000
    ExpiresByType video/mpeg A31536000
    ExpiresByType video/webm A31536000
    ExpiresByType application/vnd.ms-project A31536000
    ExpiresByType application/x-font-otf A31536000
    ExpiresByType application/vnd.ms-opentype A31536000
    ExpiresByType application/vnd.oasis.opendocument.database A31536000
    ExpiresByType application/vnd.oasis.opendocument.chart A31536000
    ExpiresByType application/vnd.oasis.opendocument.formula A31536000
```

```
   ExpiresByType application/vnd.oasis.opendocument.graphics A31536000
   ExpiresByType application/vnd.oasis.opendocument.presentation A31536000
   ExpiresByType application/vnd.oasis.opendocument.spreadsheet A31536000
   ExpiresByType application/vnd.oasis.opendocument.text A31536000
   ExpiresByType audio/ogg A31536000
   ExpiresByType application/pdf A31536000
   ExpiresByType image/png A31536000
   ExpiresByType application/vnd.ms-powerpoint A31536000
   ExpiresByType audio/x-realaudio A31536000
   ExpiresByType image/svg+xml A31536000
   ExpiresByType application/x-shockwave-flash A31536000
   ExpiresByType application/x-tar A31536000
   ExpiresByType image/tiff A31536000
   ExpiresByType application/x-font-ttf A31536000
   ExpiresByType application/vnd.ms-opentype A31536000
   ExpiresByType audio/wav A31536000
   ExpiresByType audio/wma A31536000
   ExpiresByType application/vnd.ms-write A31536000
   ExpiresByType application/font-woff A31536000
   ExpiresByType application/font-woff2 A31536000
   ExpiresByType application/vnd.ms-excel A31536000
   ExpiresByType application/zip A31536000
</IfModule>

<IfModule mod_deflate.c>
      AddOutputFilterByType DEFLATE text/css text/x-component application/x-javascript
application/javascript text/javascript text/x-js text/html text/richtext text/plain text/xsd text/xsl text/xml
image/bmp application/java application/msword application/vnd.ms-fontobject application/x-msdownload
image/x-icon image/webp application/json application/vnd.ms-access video/webm application/vnd.ms-
project application/x-font-otf application/vnd.ms-opentype application/vnd.oasis.opendocument.database
application/vnd.oasis.opendocument.chart application/vnd.oasis.opendocument.formula
application/vnd.oasis.opendocument.graphics application/vnd.oasis.opendocument.presentation application/
vnd.oasis.opendocument.spreadsheet application/vnd.oasis.opendocument.text audio/ogg application/pdf
application/vnd.ms-powerpoint image/svg+xml application/x-shockwave-flash image/tiff application/x-font-
ttf application/vnd.ms-opentype audio/wav application/vnd.ms-write application/font-woff application/font-
woff2 application/vnd.ms-excel
<IfModule mod_mime.c>

# DEFLATE by extension
 AddOutputFilter DEFLATE js css htm html xml
</IfModule>
</IfModule>

<FilesMatch "\.(css|htc|less|js|js2|js3|js4|CSS|HTC|LESS|JS|JS2|JS3|JS4)$">
   FileETag MTime Size
   <IfModule mod_headers.c>
      Header unset Set-Cookie
   </IfModule>
</FilesMatch>

<FilesMatch "\.(html|htm|rtf|rtx|txt|xsd|xsl|xml|HTML|HTM|RTF|RTX|TXT|XSD|XSL|XML)$">
   FileETag MTime Size
   <IfModule mod_headers.c>
      Header append Vary User-Agent env=!dont-vary
   </IfModule>

</FilesMatch>
```

```
<FilesMatch "\.(asf|asx|wax|wmv|wmx|avi|bmp|class|divx|doc|docx|eot|exe|gif|gz|gzip|ico|jpg|jpeg|jpe|
webp|json|mdb|mid|midi|mov|qt|mp3|m4a|mp4|m4v|mpeg|mpg|mpe|webm|mpp|otf|_otf|odb|odc|odf|
odg|odp|ods|odt|ogg|pdf|png|pot|pps|ppt|pptx|ra|ram|svg|svgz|swf|tar|tif|tiff|ttf|ttc|_ttf|wav|wma|wri|
woff|woff2|xla|xls|xlsx|xlt|xlw|zip|ASF|ASX|WAX|WMV|WMX|AVI|BMP|CLASS|DIVX|DOC|DOCX|EOT|EXE|
GIF|GZ|GZIP|ICO|JPG|JPEG|JPE|WEBP|JSON|MDB|MID|MIDI|MOV|QT|MP3|M4A|MP4|M4V|MPEG|MPG|
MPE|WEBM|MPP|OTF|_OTF|ODB|ODC|ODF|ODG|ODP|ODS|ODT|OGG|PDF|PNG|POT|PPS|PPT|PPTX|RA|
RAM|SVG|SVGZ|SWF|TAR|TIF|TIFF|TTF|TTC|_TTF|WAV|WMA|WRI|WOFF|WOFF2|XLA|XLS|XLSX|XLT|
XLW|ZIP)$">
   FileETag MTime Size
   <IfModule mod_headers.c>
      Header unset Set-Cookie
   </IfModule>
</FilesMatch>

<FilesMatch "\.(bmp|class|doc|docx|eot|exe|ico|webp|json|mdb|webm|mpp|otf|_otf|odb|odc|odf|odg|odp|
ods|odt|ogg|pdf|pot|pps|ppt|pptx|svg|svgz|swf|tif|tiff|ttf|ttc|_ttf|wav|wri|woff|woff2|xla|xls|xlsx|xlt|xlw|
BMP|CLASS|DOC|DOCX|EOT|EXE|ICO|WEBP|JSON|MDB|WEBM|MPP|OTF|_OTF|ODB|ODC|ODF|ODG|ODP|
ODS|ODT|OGG|PDF|POT|PPS|PPT|PPTX|SVG|SVGZ|SWF|TIF|TIFF|TTF|TTC|_TTF|WAV|WRI|WOFF|
WOFF2|XLA|XLS|XLSX|XLT|XLW)$">
   <IfModule mod_headers.c>
      Header unset Last-Modified
   </IfModule>

</FilesMatch>
<IfModule mod_headers.c>
   Header set Referrer-Policy "no-referrer-when-downgrade"
</IfModule>

# END W3TC Browser Cache
# BEGIN W3TC CDN
<IfModule mod_headers.c>
   Header set Access-Control-Allow-Origin "*"
</IfModule>

# END W3TC CDN

# BEGIN W3TC Page Cache core
<IfModule mod_rewrite.c>
   RewriteEngine On
   RewriteBase /
   RewriteRule ^(.*\/)?w3tc_rewrite_test([0-9]+)/?$ $1?w3tc_rewrite_test=1 [L]
   RewriteCond %{HTTPS} =on
   RewriteRule .* - [E=W3TC_SSL:_ssl]
   RewriteCond %{SERVER_PORT} =443
   RewriteRule .* - [E=W3TC_SSL:_ssl]
   RewriteCond %{HTTP:X-Forwarded-Proto} =https [NC]
   RewriteRule .* - [E=W3TC_SSL:_ssl]
   RewriteCond %{HTTP:Accept-Encoding} gzip
   RewriteRule .* - [E=W3TC_ENC:_gzip]
   RewriteCond %{HTTP_COOKIE} w3tc_preview [NC]
   RewriteRule .* - [E=W3TC_PREVIEW:_preview]
   RewriteCond %{REQUEST_METHOD} !=POST
   RewriteCond %{QUERY_STRING} =""
   RewriteCond %{HTTP_COOKIE} !(comment_author|wp\-postpass|w3tc_logged_out|
wordpress_logged_in|wptouch_switch_toggle) [NC]
   RewriteCond %{REQUEST_URI} \/$
   RewriteCond "%{DOCUMENT_ROOT}/wp-content/cache/page_enhanced/%{HTTP_HOST}/
```

```
{REQUEST_URI}/_index%{ENV:W3TC_SSL}%{ENV:W3TC_PREVIEW}.html%{ENV:W3TC_ENC}" -F
    RewriteRule .* "/wp-content/cache/page_enhanced/%{HTTP_HOST}/%{REQUEST_URI}/_index%
{ENV:W3TC_SSL}%{ENV:W3TC_PREVIEW}.html%{ENV:W3TC_ENC}" [L]
</IfModule>
# END W3TC Page Cache core

# BEGIN ShortPixelWebp
# END ShortPixelWebp
php_flag
 zlib.output_compression off
```

Personalizações de Proteções Essenciais

```
# Prevenindo listagem de diretórios
Options All -Indexes
```

 # Previnindo tráfego malicioso Script Injection

```
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (<|%3C).*script.*(>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|[|%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|[|%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]
```

 # Bloquear acesso direto arquivos PHP plugins:

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?colomboprevidencia.com.br [NC]
RewriteRule \.(jpg|jpeg|png|gif)$ - [NC,F,L]
RewriteRule wp-content/plugins/(.*\.php)$ - [R=404,L]
```

 # Usando páginas de erros personalizadas

```
ErrorDocument 403 https://www.hostcuritiba.net.br/protecao-websites.html
ErrorDocument 400 https://www.hostcuritiba.net.br/protecao-websites.html
ErrorDocument 401 https://www.hostcuritiba.net.br/protecao-websites.html
ErrorDocument 403 https://www.hostcuritiba.net.br/protecao-websites.html
ErrorDocument 500 https://www.hostcuritiba.net.br/protecao-websites.html
```

 # Protegendo o arquivo wp-config.php

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

 # Protegendo o arquivo .htaccess

```
<files ~ "^.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</files>
```

 # Compressão via .htaccess

```
<ifmodule mod_gzip.c="">
mod_gzip_on  Yes
mod_gzip_dechunk  Yes
mod_gzip_item_include file      \.(html?|css|js|php|pl)$
mod_gzip_item_include handler   ^cgi-script$
mod_gzip_item_include mime      ^text/.*
mod_gzip_item_include mime      ^application/x-javascript.*
```

```
mod_gzip_item_exclude mime      ^image/.*
mod_gzip_item_exclude rspheader ^Content-Encoding:.*gzip.*
</ifmodule>
```

 # Preservando cache navegador

```
<IfModule mod_expires.c>
ExpiresActive On
ExpiresByType image/jpg "access 1 year"
ExpiresByType image/jpeg "access 1 year"
ExpiresByType image/gif "access 1 year"
ExpiresByType image/png "access 1 year"
ExpiresByType text/css "access 1 month"
ExpiresByType application/pdf "access 1 month"
ExpiresByType text/x-javascript "access 1 month"
ExpiresByType application/x-shockwave-flash "access 1 month"
ExpiresByType image/x-icon "access 1 year"
ExpiresDefault "access 2 days"
</IfModule>

# Wordfence WAF
<Files ".user.ini">
<IfModule mod_authz_core.c>
        Require all denied
</IfModule>
<IfModule !mod_authz_core.c>
        Order deny,allow
        Deny from all
</IfModule>
</Files>

# END Wordfence WAF

# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```

Também é importante a sua rede local não salvar senhas em navegadores que automatizam o acesso, e ao usar software FTP para envio de aquivos apenas com protocolos de SSL SFTP dê preferência no aprendizado de envios direto pelo navegador via gerenciador de arquivos do cPanel.

Medidas de prevenção locais e on-line no wp garantem que seu site esteja sempre seguro, caso contrário, não haveria grandes portais de negócios por anos com o wp desde a versão 5.1.x e isso é garantido e não use versões anteriores e vulneráveis.

Curitiba. 15/01/2020