



Inovando a cada instante

As orientações aqui presentes são em sua maioria para o CMS Joomla e Servidores Linux, em sua última versão em produção 2016. Mas também podem servir para outros CMS's. Não obstante, preste bastante atenção ao fazer suas alterações e, consulte a documentação de seu CMS favorito. Este pequeno guia não se responsabiliza pelas alterações inadequadas que você usuário faz em seu CMS.

→ **OBS:** **Imprima** essas dicas e, use-as como o seu **CheckList** ao desenvolver com o Joomla.



CheckList de Segurança no Joomla 3

- 1) → Consertar a base do banco de dados instalado após a instalação do Joomla : Extensões > Gerenciar > Banco de Dados > "Corrigir".
- 2) → Manter o sistema sempre atualizado.
- 3) → Desabilite o relatório de erros pois eles pesam o seu website e mostram aos possíveis invasores, as falhas de segurança do seu website. Para desabilitar o relatório basta seguir a seguinte sequência: Configurações Globais – Sistema – Relatório de Erros -> nenhum;
- 4) → Barrar o diretório /administrator, pode ser feito com o arquivo ".htaccess" e senha. MAS preste atenção ! Mantenha o cabeçario original que o Joomla gera quando é instalado. Caso o contrário seja removido, dará erro 500 ("Internal Server Error"), e praticamente seu site ficará travado e sem segurança.
- 5) → As versões **1.5.xx, 1.6.xx e, 1.7.xx** do Joomla, já estão **sem suporte** há bastantes anos ! Use sempre as mais recentes, a partir do Joomla 3.3.6 ou superior ! Muitas melhorias foram implementadas, inclusive na questão de segurança.
- 6) → Ter e fazer um backup do seu Site sempre : Tanto dos arquivos do Site, quanto do Banco de Dados. Pode se utilizar o "Akeeba Backup".
- 7) → Ofuscar o diretório /administrator com plugins. Alguns plugins danificam o joomla, em algumas atualizações do joomla.
- 8) → AdminExile : Um redirecionador que gera um link com um token alternativo que só você tem acesso e, é através dele que você acessa seu painel de login para ir no painel de controle do Joomla. (<http://extensions.joomla.org/extension/adminexile>)
- 9) → Alterar o nome de usuário "admin" para outro usuário superadministrador.
- 10) → Fazer senhas complexas/fortes para o superadministrador, inclusive com caracteres especiais ("!@#\$\$%*()_+^"), letras e números (Maiusculos e minusculos).
Ex : "\$\$tvwfj4564@s2!^fDs#".
Site gerador de senhas complexas : <https://identitysafe.norton.com/pt-br/password-generator>

- 11)→ Instalar plugins de dupla autenticação ou autenticação de dois fatores. Quanto mais camadas, melhor. Mas aumenta as suas chances de errar durante o processo de login. Exemplo : http://en.wikipedia.org/wiki/Google_Authenticator/ / <https://support.google.com/accounts/answer/1066447?hl=en>
- 12)→ Salvar todos os seus dados de acesso em um pendrive e, use-o em um computador que não seja Windows.
- 13)→ Instalar plugin para evitar ataques MySQL Injection. Há plugins que te avisam via email sobre tentativas de ataques.
- 14)→ Plugin que avisa por email novas atualizações do Joomla.
- 15)→ Instalar componente, plugin de UpDate automático do Joomla. (<https://www.siteground.com/tutorials/joomla/joomla-autoupdate.htm>) e (<http://www.templatemonster.com/help/joomla-3-x-automatic-engine-update.html#gref>)
- 16)→ Procurar hospedagem de sites que possuem sistemas de defesa de ataques DoS ou DDoS ou DRDoS e que mostrem os IPs que mais acessam seu site e diretórios.
- 17)→ Desabilitar módulos de login de usuários, deixá-los despublicados ou desinstalados. Exemplo :
`GET 404 /component/users/?view=login&return=aHR0cDovL3Byb3NlZ2JoLmNvbS5ici9pbmRleC5waHA/b3B0aW9uPWNvbV9waG9jYWVvd25sb2FkLnZpZXc9Y2F0ZWdvcnkmcZG93bmxvYWQ9MTg6YXZlbnRhaXMtZS1sdXZhc31lbS10aGVyYbW9jcm9uLWlnbmlmdWdvLWF0ZS0yNTBvLWNhdC04LTkmaWQ9NDpwZXJpc3NhdG8=`
 Ou :
</component/mailto/?tmpl=component&template=allrounder-j1.6&link=31a090ce209f02470a4e91b98467838ecf871201>
- 18)→ Verificar se o template é elegível para o uso em um site de produção. Se não há históricos de códigos maliciosos em seu sistema de template ou framework. Também, após isso, e testar um tanto de templates, remova/desinstale os que você não vai usar. "Há algum motivo para manter sua roupa antiga?" Não use template pirata.
- 19)→ Mover o arquivo "configuration.php". Prestar atenção quando for atualizar o Joomla ! Sugestão : (<http://vel.joomla.org/articles/275-moving-the-configuration-php-file>).
- 20)→ Há extensões que são pagas que são melhores, mas há extensões gratuitas que também dão conta do "recado".
- 21)→ As permissões chmod para diretório são "0755" e para arquivos são "0644". Verificar se estão assim.
- 22)→ Instalar o seu Joomla sempre dos "MagicsBox" ou "ToolsBox"(Scripts pré-instalados). Desenvolver o site sempre no servidor que vai estar em produção, para garantir as configurações das permissões de diretórios e, arquivos padrões do sistema de hospedagem.
- 23)→ Link Oficial para o "Security Checklist" : https://docs.joomla.org/Security_Checklist
- 24)→ Link Oficial para a "A Few Basic Security Rules" : <http://vel.joomla.org/articles/1632-a-few-basic-security-rules>
- 25)→ Ocultar o <meta name="generator" content="Joomla XXX" /> no Joomla 3.

"Exemplo :

- Acesse o seu FTP e vá até a pasta /libraries/joomla/document/html/renderer;
- Baixe o arquivo "head.php";
- No Joomla 3.x procure o comentário `"/ Don't add empty generators"` em :
`($buffer .= $tab . '<meta name="generator" content="'. htmlspecialchars($generator) . "' />'. $lnEnd);`
- Renomeie como quiser a linha alterando o `content="CONTEÚDO QUE QUISER"`;
- Salve o arquivo e suba no FTP novamente.

O mesmo com o campo `// Don't add empty descriptions .`

”

*** No entanto, parece que não está funcionando. Então, caso não funcione, será necessário o uso de algum extensão que altere esses campos.**

26)→ Usar o sistema de captcha, também em formulários.


Exemplo :

<http://extensions.joomla.org/extensions/extension/contacts-and-feedback/forms/chronoforms>

<http://extensions.joomla.org/extension/keycaptcha>

27)→ Caso não queira usar as extensões de formulário de contato : Use algum gratuito online ou, hospede seu formulário de contato em outra conta ou servidor, assim se evita *injections*, e um controle melhor na identificação de problemas com formulários de contato.

28)→ "Site offline" : Usar alguma extensão para descaracterizar a página pública principal e, sem os campos de acesso ao usuário como "user" e "senha". Ao despublicar os campos de formulário de login "user" e "senha" evita-se o MySQL Injection nesses campos. Ex : (<http://extensions.joomla.org/extensions/extension/miscellaneous/offline/ig-offline-page>).

29)→ Altere o "favicon" (<http://www.etc...>) padrão do Joomla, removendo-o ou alterando para algum "favicon" de sua preferência. Alguns plugins ou componentes fazem isso.

30)→ De costume, sempre verifique os códigos das extensões que você usa. É só abrir o arquivo compactado e verificar. Após, recomprima o arquivo em ".zip".

31)→ Habilite as opções "Adicionar sufixo de URL" e "Utilizar mod_rewrite" nas "Configurações globais".

32)→ Configure as URLs amigáveis nas configurações globais.

33)→ Desabilite algumas funções vulneráveis do PHP : `disable_functions = show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open`. Verifique com o arquivo "teste.php" com o código `<?php phpinfo(); ?>` . Isso mostrará as configurações do php em seu servidor. O Joomla também exibe isso na parte de configurações na administração.

34)→ Desativar RG_EMULATION . Consultar seu Provedor de Hospedagem, caso não tenha acesso.

35)→ Dê preferência, use o Linux ou MacOS para administrar o seu Joomla, assim pode evitar que vírus monitorem seu acesso ao Joomla.

36)→ Conceda apenas os privilégios necessários ao usuário do banco (Mysql).

37)→ Integre o seu site com o CloudFlare para proteja-lo contra ataques DoS ou DDoS ou DRDoS e IPs reconhecidamente considerados como fonte de ataques (<https://www.cloudflare.com/ddos>).

38)→ Bloquear IPs com tentativas de invasão. Pode ser feito : Através do ".htaccess" com a função, exemplo :

"

Order Deny,Allow

Deny from xxx.xxx.xxx.xxx

"

Ou, através do painel de controle de sua hospedagem. Há recursos mais avançados a nível de acesso remoto (SSH) que capturam esses e-mails com tentativas de invasão, e mostram o diretório que foi o acesso/tentativa.

39)→ Caso no futuro precise mudar a senha porque esqueceu-a, acesse o seu gerenciador de banco de dados (Terminal SSH > MySQL, ou phpmyadmin). Em *users*, edite, e seta para o tipo MD5 que é para criptografia da senha no MySQL.

40)→ Alguns links comumente usados para tentativas de SQL Injection :

<http://SeuSite/component/users/?view=remind>

<http://SeuSite/component/users/>

41)→ Plugins > “User – Joomla!” > “Auto-criar Usuários”. Por padrão vem “Sim” (habilitado). Desmarcar e, colocar na opção “Não”. (TESTE antes de fazer isso.).

42)→ Instalar extensões de Firewalls, proteção da Administração, como por exemplo :

- Centora Security TM,
- DMC Firewall,
- AdminTools,
- Securitycheck,
- SQL Injection Marcos Interceptor,
- jHackGuard,
- RS Firewall,
- aeSecure's QuickIcon Administration (<http://extensions.joomla.org/extensions/extension/access-a-security/aesecure-s-quickicon-administration-module>)

* Também sempre note se a extensão é bem utilizada e, atualizada constantemente no site <http://extensions.joomla.org> .

Exemplo :

Akeeba Backup

Version: 5.1.0
Developer: [Akeeba Ltd](#)
Last updated: Jul 05 2016
Date added: Jun 05 2007
License: [GPLv2 or later](#)
Type: Free download
Uses updater:

Includes:
Compatibility:

[Download](#) [Demo](#) (Not available)
[Support](#) [Documentation](#)

Overall: 100
Functionality: 100
Ease of use: 100
Documentation: 100

43)→ Caso tenha acesso de instalação de programas em seu servidor, seja uma VPN ou Cloud VPN, ou servidor alugado, é interessante instalar programas antivírus para o Linux e específicos para a varredura de sites. Para isso existe o Nikto2, que é um antivírus para administradores de CMS, como o Joomla, que faz uma varredura nos CMS. (<https://cirt.net/Nikto2>).

Temos também o ClamV, que é um antivírus para o sistema operacional Linux. (<http://www.clamav.net>).

44)→ **Teste de segurança no Joomla :**

Projetos : nikto, joomscan, owasp, sucuri, netsparker.

<http://www.beyondsecurity.com>,
<https://www.acunetix.com>,
<http://sitecheck.sucuri.net>
<https://www.netsparker.com/>

**Alguns são gratuitos, mas outros são pagos.*

45)→ Antivirus Website Protection : Um antivírus para o Joomla. Possui a versão free e a versão paga. Na versão free esse componente funciona em modo trial de 14 dias. (<http://extensions.joomla.org/extensions/extension/access-a-security/site-security/antivirus-website-protection>)

46)→ Faça testes em seu site usando programas e distribuições Linux que já vêm com muitos programas, como a distribuição Linux Back|Track. (<http://www.backtrack-linux.org/>)

→ Adendo :

Mais informações sobre como melhorar a segurança do Joomla, no site Oficial :
<https://docs.joomla.org/Security>

Lista de componentes inseguros (Joomla! ® Vulnerable Extensions List) :
<https://vel.joomla.org/index.php/live-vel>

→ Sites baseados para as dicas acima :

<https://www.security.unicamp.br/artigos/22-dicas-seguranca-joomla.html>
<http://www.frhost.com.br/blog/seguranca/seguranca-joomla-tornando-o-joomla-mais-seguro>
<http://www.joomlabr.org/alterando-a-meta-tag-generator-do-joomla>
<http://www.webmaster.pt/joomla-tutorial-seguranca-4.html>
<http://forum.joomla.org/viewforum.php?f=374>
<http://www.melhorweb.com.br/artigo/687-Como-melhorar-a-seguranca-no-Joomla-r.htm>
<http://www.criarweb.com/artigos/seguranca-joomla.html>

→ Templates :

<http://www.joomlabr.org/templates-joomla-free-onde-consigo>

→ **Teste de segurança no Joomla :**

Extensões : nikto, joomscan, sucuri

<http://www.beyondsecurity.com>,

<https://www.acunetix.com>,

<http://sitecheck.sucuri.net>

<https://www.netsparker.com/>

→ **LICENÇA :**



*O autor incentiva qualquer correção e implementação pela comunidade.
Este pequeno guia é livre e, não possui em qualquer hipótese de diretivas comerciais.*

É um presente para a Comunidade !
