

Empresa de Informática e Informação do Município de Belo Horizonte S/A

**PRODABEL**

**Gerência:** GGSS

**Projeto:** Autorização Alvará Simplificado

**Cliente:** SMSA

**Plano de Implantação**

**Autor: Samuel Silva Taveira**

**Belo Horizonte, maio de 2018**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **IDENTIFICAÇÃO** *[Responsável pelo preenchimento: gerente do projeto]* | | | | | | | |
| **Projeto ou Sistema** | Sistema de Autorização de Alvará Simplificado | | | | **Sigla** | AAS | |
| **Unidade Responsável pelo Projeto** | GGSS | | **Nome Contato/ Ramal** | | Samuel Taveira/74337 | | |
| **Unidade Responsável pela Sustentação** | GGSS | | **Nome Contato/ Ramal** | | Samuel Taveira / 4337 | | |
| **Área temática** | Saúde | | | | | | |
| **Produto** | Autorização do Alvará Simplificado | | | | | | |
| **Identificador numérico do Sistema no GSS – Gestão de sistemas em sustentação** | 1001296 | | | | | | |
| **URL do Repositório** | https://gitlab.pbh.gov.br/saude/sisvisa | | | | | | |
| **URL do Sistema*[[1]](#footnote-0)*** | http://aas-hm.pbh.gov.br | | | | | | |
| **Tipo de acesso à URL** | ☐  **Interna (RMI)** | ☒  **Externa (Internet)** | | | ☐  **Ambos (RMI/Internet)** | | |
| **Ambiente** | ☐ **Desenvolvimento** | | | ☒ **Homologação/Teste** | | | ☐ **Produção** |
| **Outro :** ambiente em PHP 7.1 | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **MOTIVAÇÃO/OBJETIVO** *[Responsável pelo preenchimento: gerente do projeto]* | | | | |
| ☒ **Inicial** | ☒ **Atualização** | ☐ **Evolução** | ☐ **Correção** | **Crítica?**  ☐ **S**im  ☐ **N**ão |
| **Criação do Sistema para a Autorização de Alvará Sanitário Simplificado** | | | | |
|  | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **ITENS DE CONFIGURAÇÃO DO PRODUTO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor/GSOI]* | | | |
|  | ***Corrente*** | ***Nova*** | |
| **Produto** [gerente do projeto/fornecedor] | N/A | Sistema de Autorização de Alvará Sanitário Simplificado | |
| **Versão do Produto** [gerente do projeto/fornecedor] | N/A | 1.0 | |
| **Servidor\*** [GSOI] | [hostname corrente] | N/A | |
| **Versão SNMP e *Community\**** [GSOI] | [versão do protocolo SNMP e *community* utilizada] | N/A | |
| **Discos\*** [GSOI] | [discos a serem monitorados e seus respectivos *thresholds*] | [discos a serem monitorados e seus respectivos *thresholds*] | |
| **Processos\*** [GSOI] | [nome dos processos a serem monitorados] | [nome dos processos a serem monitorados] | |
| **IP Address** [GSOI] | N/A | [endereço IP novo] | |
| **Sistema operacional  (SO)** [gerente do projeto/fornecedor] | N/A | linux | |
| N/A | Debian 7 | |

\* O preenchimento das informações permite o monitoramento básico e obrigatório de falhas e performance das máquinas.

|  |  |  |
| --- | --- | --- |
| 1. **OUTROS ITENS DE CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* | | |
|  | ***Corrente*** | ***Nova*** |
| **Servidor Web*[[2]](#footnote-1)*** | N/A | Apache |
| N/A | 2.4.27 |
| N/A | N/A |
| **Web Engine*[[3]](#footnote-2)*** | N/A | PHP |
| N/A | 7.1 |
| **Servidor de Aplicação*[[4]](#footnote-3)*** | N/A | N/A |
| N/A | N/A |
| **Web Container*[[5]](#footnote-4)*** | N/A | N/A |
| N/A | N/A |
| N/A | N/A |
| **Persistência (SGBD)** | N/A | Sql Server |
| N/A | 2008 |
| N/A | |  |  | | --- | --- | |  | MSSQLPR01  /VISA2/VISA2 | |
| **Requisitos computadores Clientes** | N/A | N/A |
| N/A | N/A |
| **Outros produtos / bibliotecas** | N/A | OpenSSL PHP Extension |
| N/A | PDO PHP Extension |
| N/A | Mbstring PHP Extension |
| N/A | Tokenizer PHP Extension |
| N/A | XML PHP Extension |
| N/A | php\_pdo\_sqlsrv\_71\_ts\_x86.dll |
| N/A | php\_oci8\_11g.dll |
| N/A | Módulos Apache: mod\_rewrite |

|  |  |  |
| --- | --- | --- |
| 1. **PLATAFORMA DE DESENVOLVIMENTO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* | | |
| **[Linguagem utilizada]** | **[Plataforma operacional]** | **[Ferramenta de Desenvolvimento]** |
| PHP | Linux | LARAVEL 5.5 |

|  |  |  |
| --- | --- | --- |
| 1. **REQUISITOS DE HARDWARE ESTAÇÃO CLIENTE CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* | | |
| **[Processador]** | **[Memória]** | **[Espaço em Disco]** |
| N/a | N/a | N/a |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **REQUISITOS DE AMBIENTE DE HOMOLOGAÇÃO/PRODUÇÃO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* | | | |
| **[Homologação/**  **Produção]** | **[Processador]** | **[Memória - mínimo]** | **[Espaço em Disco para Instalação]** |
| Homologação | 2 Processadores | 2gb | 1gb |

|  |
| --- |
| 1. **RELAÇÃO DE SERVIÇOS DISPONIBILIZADOS PELA APLICAÇÃO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| **[nome do serviço (irá compor o catálogo de serviços]** |
| http://aas-hm.pbh.gov.br |

\* O monitoramento básico das máquinas está contemplado no processo de implantação. No caso de necessidade de qualquer monitoração refinada, deverá ser preenchido o Plano de Monitoração.

|  |
| --- |
| 1. **PRÉ-CONDIÇÕES CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| **[circunstâncias que devem anteceder a implantação]** |
| **Módulos PHP para o Laravel Funcionar:**  OpenSSL PHP Extension  PDO PHP Extension  Mbstring PHP Extension  Tokenizer PHP Extension  XML PHP Extension  php\_oci8\_11g.dll  php\_pdo\_sqlsrv\_71\_ts\_x86.dll  php\_soap.dll  **Módulos Apache:**  mod\_rewrite  As pastas /bootstrap/cache/ e /storage devem possuir permissão 775 e pertencerem ao mesmo grupo e serem do do usuário do apache que é geralmente o www-data. Caso não tenha essas permissões um erro de permissão será exibido pela aplicação. |

|  |
| --- |
| 1. **PÓS-CONDIÇÕES CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| **[situações que confirmem o sucesso da implantação]** |
| N/A |

|  |
| --- |
| 1. **PROCEDIMENTO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| **[descrição resumida de passos][[6]](#footnote-5)** |
| 1. Após a configuração do ambiente habilitar as bibliotecas citadas no plano 2. Criar a url http://aas-hm.pbh.gov.br 3. Copiar os fontes da aplicação:   O caminho no servidor publicaversao.pbh/ /softwares/InfraEstrutura/Builds/SISVISA2/homologacao/20180509   1. Publicar a aplicação no servidor apache. |

|  |
| --- |
| 1. **RETORNO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| [descrição das ações de retorno em caso de insucesso da implantação] |
| Interromper a implantação e informar ao analista responsável os problemas. |

|  |  |
| --- | --- |
| 1. **CONTINGÊNCIA CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* | |
| **[descrição da possível falha]** | **[descrição da ação de contorno]** |
| Problema na criação do ambiente da aplicação. | Entrar em contato com o Samuel Taveira |

|  |
| --- |
| 1. **ESTIMATIVA DE TEMPO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| [estimar tempo gasto para cada tarefa] |
|  |

|  |
| --- |
| 1. **DOCUMENTAÇÃO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| **[referencia a documentação adicional em anexo e/ou manuais de procedimentos detalhados – passo-a-passo – de implantação / geração de build e processo de deployment]** |
| N/A |

|  |
| --- |
| 1. **SEGURANÇA CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| **[Rotinas e procedimentos de segurança adotados na aplicação tais como: procedimento de autenticação, autorização, certificação etc..]** |
| **Usar o serviço de autenticação e autorização de acesso [ ]** |
| N/A |

|  |
| --- |
| 1. **DECLARAÇÃO CONFIGURAÇÃO** *[Responsável pelo preenchimento: gerente do projeto/fornecedor]* |
| **Declaro estar ciente das diretrizes de segurança para implantação de sistemas web no ambiente de produção da Prodabel referenciadas no anexo II deste documento e que este sistema cumpre estas diretrizes integralmente.**  **Belo Horizonte, 09 de maio de 2017**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |  |  |
| --- | --- | --- |
| 1. **REVISÕES DO ARTEFATO** | | |
| **Data** | **Descrição** | **Responsável** |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **APROVAÇÃO** | | | |
| **Orgão/Setor** | **Nome** | **Data** | **Assinatura** |
|  |  |  |  |

**ANEXO I**

1. **PRÉ-CONDIÇÕES PARA IMPLANTAÇÃO DE SISTEMAS EM PRODUÇÃO**
   1. Ter o Plano de Implantação aprovado.
   2. Ter a Requisição de Mudanças - RDM Aprovada. O Responsável pelo sistema deverá encaminhar uma solicitações de mudança através do formulário de Requisição de Mudança – RDM (Anexo II) para à Gerência de Mudança, GUST–PB, através do endereço eletrônico [***mudanca@pbh.gov.br***](mailto:mudanca@pbh.gov.br). (Instrução I009 de 18/11/2009 – Instrução Normativa do Processo do Gerenciamento de Mudanças). A partir da RDM será elaborado todo o planejamento da implantação.
   3. Ter os códigos fontes carregados no repositório do software de controle de versões Subversion. Caso a aplicação ainda não tenha o repositório criado, a demanda deve ser relatada no projeto “Criação de repositório” acompanhada do formulário   
      [***PSP - Plano de Gerência de Configuração***](http://repositorio.pbh/tecnologia_informacao/mpspdbl/trunk/docs/Processos/templates/PSP-Template-PlanoGerenciaConfiguracao.doc) encontrado no site do PSP ([***https://psp.pbh.gov.br***](https://psp.pbh.gov.br/)). A instalação da ferramenta TortoiseSVN para carregar e manter os fontes da aplicação no repositório pode ser solicitada no ramal 8686. O manual de utilização da ferramenta também está disponível no site do PSP (***Ferramentas > Gerenciamento de configuração > TortoiseSVN - controle de versões***).
   4. Ter declarado que o aplicativo cumpre todas as diretrizes de segurança indicadas no anexo II – Diretrizes de Segurança para Desenvolvimento de Aplicações WEB.

**ANEXO II**

1. **DIRETRIZES DE SEGURANÇA PARA DESENVOLVIMENTO DE APLICAÇÕES WEB**
   1. **INTRODUÇÃO**

Este documento foi produzido pela Superintendência de Arquitetura de Sistemas(SAS), Superintendência de Serviços(SST) e Superintendência de Operação(SOT) e tem como objetivo relacionar as diretrizes básicas para garantir a segurança do ambiente de produção, em relação as aplicações web, que atendem a PBH e seus órgão da administração direta e indireta. Estas diretrizes devem ser seguidas durante o desenvolvimento de todos os sistemas a serem implantados no ambiente produção, o qual é de responsabilidade da Prodabel. Durante a fase de construção do software essas diretrizes devem ser observadas e na fase de transição, quando ocorrem as transferências do sistema para um ambiente de produção. O responsável pelo desenvolvimento do sistema deverá formalizar o cumprimento destas diretrizes.

Todos os sistemas implantados em produção são passiveis de auditoria e o não cumprimento destas diretrizes acarretará no imediato bloqueio do acesso ao sistema sem aviso prévio. O bloqueio será determinado com a finalidade de prevenir ataques de softwares maliciosos bem como a exploração de vulnerabilidades eventualmente identificadas nesses sistemas. Nesse caso o responsável será formalmente comunicado do evento para que os ajustes sejam implementados permitindo o retorno do funcionamento da aplicação.

* 1. **PRÉ-REQUISITOS**

Toda aplicação deve ser devidamente identificada com as seguintes informações:

- Desenvolvedor Responsável:

- Matrícula do desenvolvedor:

- E-mail do desenvolvedor responsável:         
- Órgão de Lotação:  
- Telefone:

- Órgão responsável pela aplicação:

- Responsável no Órgão:   
- Nome da Aplicação:  
- Diretório principal:  
- Frequência de atualização:  
- Usuário de "FTP":  
- Plataforma da aplicação

* 1. **DIRETRIZES GERAIS DE SEGURANÇA**
     1. **Gravação de arquivos**

Caso a aplicação necessite gravar arquivos no servidor (upload de arquivo) ela deverá fazê-la de forma indireta através de uma área compartilhada por um NFS (Network File System). A aplicação deverá utilizar a rotina de upload de arquivos disponível no seguinte endereço do portal de arquitetura de sistemas:

<http://wiki.arquitetura.pbh/doku.php?id=docs:psp:psp_padrao_upload_php>

* + 1. **Referencias locais**

A aplicação não deve fazer referências externas, mas apenas referencias locais.

* + 1. **Uso de HTTP métodos**

A aplicação deve utilizar preferencialmente o método POST do protocolo http a fim de ocultar informações sensíveis. A implementação da aplicação deve, sempre que possível, evitar o uso do método GET. Para recebimento de formulários nunca devemos utilizar o método GET. Essa diretriz foi definida com base na experiência registrada de situações de ataque que se aproveitaram da referencia explicita a parâmetros que o método GET utiliza. Alem disso esta diretriz está fundamentada nas recomendações do W3C encontrada em <http://www.w3.org/TR/2004/REC-webarch-20041215/#safe-interaction> e <http://www.w3.org/2001/tag/doc/whenToUseGet.html>.

* + 1. **PHP - Diretiva REGISTER\_GLOBALS**

As aplicações PHP não podem ativar a diretiva REGISTER\_GLOBALS uma vez foi identificado graves problemas de vulnerabilidades quando a mesma é ativada. Este recurso é extremamente não recomendado no manual do PHP no site <http://www.php.net/manual/pt_BR/security.globals.php>

* + 1. **Parametrização da aplicação**

Os parâmetros de configuração da aplicação tais como acesso a banco de dados, devem ser centralizados em um único arquivo referenciado pelos outros fontes da aplicação.

As aplicações web desenvolvidas na plataforma Java devem delegar os parâmetros de configuração do acesso ao banco de dados para o arquivo XML do container web (Tomcat). Os detalhes dessas recomendações estão registradas no PSP através do documento [D005-PSP-Roteiro-publicacao\_Aplicacoes por equipes internas.doc](http://repositorio.pbh/tecnologia_informacao/mpspdbl/trunk/docs/Processos/roteiros/PSP-Roteiro-Tomcat_publicacao_build.doc), [D005-PSP-Roteiro-publicacao\_Aplicacoes por equipes externas.doc](http://repositorio.pbh/tecnologia_informacao/mpspdbl/trunk/docs/Processos/roteiros/PSP-Roteiro-Tomcat_publicacao_build.doc) e complementam as orientações do artefato de [PSP – Plano de Implantação](http://repositorio.pbh/tecnologia_informacao/mpspdbl/trunk/docs/Processos/templates/PSP-Template-PlanoImplantacao.doc).

* + 1. **Alteração do diretório/pacote raiz da aplicação**

O diretório ou pacote raiz da aplicação deve ser modificado e uma nova publicação em produção deverá ser feita caso ocorra um evento de falha de segurança no servidor que hospeda a aplicação.

* + 1. **Imagens e arquivos estático**

Imagens e arquivos estáticos NÃO deve estar no Tomcat pois comprometem a memória da JVM, rede e outros. Elas devem estar no servidor WEB (Apache) em um diretório específico por exemplo: /var/www/nomedaaplicacao/imagens.

* + 1. **Páginas de Cadastramento de Informações em Banco de Dados**

Aplicações que possuem funções de cadastramento de informações em banco de dados com acesso pela internet devem utilizar algum mecanismo de prevenção de ataque por robôs, por exemplo <http://pt.wikipedia.org/wiki/CAPTCHA>. Uma situação de vulnerabilidade relacionada ao uso de robôs na internet é o cadastramento de e-mail para recebimento de boletins de informações.

* + 1. **Os 10 principais riscos das aplicações Web**

As aplicações devem minimizar falhas de segurança. A OWASP divulga continuamente a lista das vulnerabilidades mais frequentes em aplicações Web. Atualmente esses riscos são:

* A1: Injection: permite a inserção e execução de código malicioso em páginas Web
* A2: Cross-Site Scripting (XSS): permite a inserção de código malicioso que depois será enviado a outros usuários
* A3: Broken Authentication and Session Management: permite recuperar dados de sessões não criptografadas e que não foram encerradas
* A4: Insecure Direct Object References: permite que o usuário modifique o acesso a objetos de uma página
* A5: Cross-Site Request Forgery (CSRF): utiliza-se um site falso para solicitar informações aos usuários **(avaliar em conjunto com a área de infraestrutura)**
* A6: Security Misconfiguration: permite explorar falhas de segurança devido a configurações incorretas **(avaliar em conjunto com a área de infraestrutura)**
* A7: Insecure Cryptographic Storage: permite recuperar as informações de acesso
* A8: Failure to Restrict URL Access: permite ao usuário analisar a existência de páginas para criar um ataque
* A9: Insufficient Transport Layer Protection: permite monitorar a rede e recuperar as informações trafegadas **(avaliar em conjunto com a área de infraestrutura)**
* A10: Unvalidated Redirects and Forwards: permite redirecionamentos através da aplicação para sites externos não confiáveis

Os problemas mais recentes devem sempre ser consultados através do link <http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>. Existe material complementar em língua portuguesa disponível em <http://repositorio.pbh/tecnologia_informacao/mpspdbl/trunk/docs/Processos/outros/PSP-Diretrizes-segurancaDesenvolvimentoAplicacoesWEB.pdf>

1. A URL sugerida deve terminar com os sufixos “.pbh.gov.br” ou apenas “.pbh” dependendo se o sistema será disponibilizado na internet ou na intranet respectivamente. O nome sugerido deve seguir o padrão estabelecido através da [RFC 1738](http://tools.ietf.org/html/rfc1738) que, entre outras coisas, estabelece que os nomes não devem possuir símbolos especiais tais como \_$-\*)(. [↑](#footnote-ref-0)
2. Por exemplo, Apache [↑](#footnote-ref-1)
3. Por exemplo, PHP, Python, Perl. [↑](#footnote-ref-2)
4. Notadamente produtos aderentes ao conceito de servidor de aplicação da plataforma Java Enterprise. Por exemplo, Jboss, Websphere, Weblogic, Borland Application Server (BAS) [↑](#footnote-ref-3)
5. Sobre o procedimento de deploy de aplicações no web container Tomcat consulte os roteiros

   <https://repositorio.pbh/tecnologia_informacao/mpspdbl/trunk/docs/Processos/roteiros/PSP-Roteiro-publicacao-Aplicacoes-por-equipes-internas.doc> ou

   <https://repositorio.pbh/tecnologia_informacao/mpspdbl/trunk/docs/Processos/roteiros/PSP-Roteiro-publicacao-Aplicacoes-por-equipes-externas.doc> [↑](#footnote-ref-4)
6. Caso tenha alguma configuração para acesso ao banco de dados, favor informa a solicitação (SDM) em que foi solicitado a criação do banco de dados. [↑](#footnote-ref-5)