**Joga Fácil – Aplicativo Mobile**

**Documento de Visão**

**Versão 1.0**

|  |  |  |  |
| --- | --- | --- | --- |
| **Histórico de Revisões** | | | |
| **Versão** | **Data** | **Descrição** | **Autor** |
| 1.0 | 13/04/2016 | Criação do documento | Zulmira Monteiro Ximenes |

**Sumário**

[1. Introdução 4](#_Toc480989033)

[2. Problema 4](#_Toc480989034)

[3. Usuários 5](#_Toc480989035)

[4. Visão Geral do Produto 14](#_Toc480989036)

[5. Características do Produto 14](#_Toc480989037)

[6. Interface com Outros Sistemas 27](#_Toc480989038)

[7. Restrições Impostas 27](#_Toc480989039)

[8. Precedência e Prioridade 28](#_Toc480989040)

[9. Requisitos de Documentação 28](#_Toc480989041)

[10. Anexos 29](#_Toc480989042)

[11. Referências 29](#_Toc480989043)

[12. Aprovações 29](#_Toc480989044)

**Documento de Visão**

# Introdução

O objetivo deste documento é coletar, analisar e definir as características e necessidades de alto nível do sistema SSA – Sistema de Segurança de Aplicações, descrevendo os módulos de Autenticação, Autorização e Auditoria. Os detalhes de como o SSA – atende estas necessidades estão detalhados na especificação de caso de uso.

# Problema

Atualmente o CLIENTE não possui controle de acesso unificado aos sistemas, contribuindo para a falta de segurança na autenticação de usuários, restrições ao acesso das funcionalidades e monitoramento das ações realizadas pelos usuários nos sistemas.

## Resumo do Negócio

O CLIENTE necessita de controle de acesso de forma unificada aos demais sistemas, garantindo a autenticação, autorização e auditoria dos usuários.

## Problemas

|  |  |
| --- | --- |
| **O problema de** | Falta de acesso centralizado dos sistemas. |
| **Afeta** | Os usuários dos sistemas do CLIENTE. |
| **Cujo impacto é** | Falha de segurança na autenticação de usuários. |
| **Benefícios de uma solução seriam** | Permitir que os usuários previamente cadastrados possam ser autenticados por meio de um provedor de identidades apenas uma vez e a partir da autenticação ter acesso aos sistemas para os quais possuam permissão. |

|  |  |
| --- | --- |
| **O problema de** | Falta de permissões de acesso aos usuários autenticados. |
| **Afeta** | Os usuários dos sistemas do CLIENTE. |
| **Cujo impacto é** | Impedir a aplicação de política de restrições ao acesso das funcionalidades dos sistemas. |
| **Benefícios de uma solução seriam** | Autorizar o acesso dos usuários às funcionalidades dos sistemas através das permissões de segurança. |

|  |  |
| --- | --- |
| **O problema de** | Falta de monitoramento das ações realizadas nos sistemas. |
| **Afeta** | Os usuários dos sistemas do CLIENTE. |
| **Cujo impacto é** | Falha no rastreamento das ações realizadas pelos usuários nos sistemas. |
| **Benefícios de uma solução seriam** | Garantir a segurança e a integridade dos dados dos sistemas através do monitoramento das ações realizadas pelos usuários. |

# Usuários

## Resumo dos Usuários

|  |  |  |
| --- | --- | --- |
| **Nome** | **Descrição** | **Responsabilidades** |
| Coordenação de Tecnologia da Informação | Administrador do sistema. | Atribuir permissões de administradores de Unidades às respectivas chefias.  Atribuir permissões de operador de Unidades à equipe de Suporte ao Usuário. |
| Coordenadores ou Chefes de Serviços das Unidades do CLIENTE. | Representante de uma Unidade, que possua algum cargo de chefia. | Criar e atribuir permissões de acesso para sua área ou Unidade. |
| Área de Suporte ao Usuário (Help Desk – Call Center) | Prestadores de serviços de empresa contratada para as funções de suporte ao usuário. | Atribuir permissões de acesso para área ou Unidade sob solicitação da mesma. |

## Ambiente do Usuário

O APP Joga Fácil – Aplicativo Mobile para reserva de campos de futebol depende: ! Aplicações que foram acessadas a partir da sessão iniciada na estação do usuário e tenham sido construídas para usar os recursos do APP. Caso não necessite dessa propagação, o sistema pode ser acessado de qualquer sistema operacional, neste caso, a propagação será entre os sistemas que tenham sido construídos com o suporte ao APP.

## Necessidades dos Interessados

|  |  |
| --- | --- |
| Crítico | Requisitos essenciais ou o fracasso em sua implementação significa que o sistema não irá atender as necessidades do cliente. Imprescindível que seja atendido pelo sistema, condição fundamental para o sucesso do projeto. |
| Importante | Requisitos importantes para a eficácia ou eficiência do sistema. Sua não implementação afeta a satisfação do usuário e/ou o valor agregado do produto. Afeta a satisfação do usuário significativamente, mas o não atendimento não determina o fracasso do projeto. |
| Útil | Requisitos úteis, porém, menos críticos, sendo usados menos frequentemente. Não possui muito significado para a satisfação do usuário e pode deixar de ser atendida. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Necessidade** | **Prioridade** | **Preocupações** | **Solução Atual** | **Soluções Propostas** |
| 1. O APP necessita conceder acesso dos usuários aos sistemas. | Crítico | Controlar as reservas dos campos | A autenticação individual atualmente não atende aos requisitos de segurança. | Permitir que os usuários previamente cadastrados possam se autenticar apenas uma vez e a partir da autenticação ter acesso aos perfis para os quais possuam permissão. |
| 1. O APP necessita prover aos usuários a redefinição de senhas de acesso partir do conjunto de informações pré-definidas. | Importante | Redefinir senhas de acesso dos sistemas. | N/A | Permitir redefinir senhas de acesso a partir de um dos seguintes conjuntos de informações pré-definidas: utilizando os dados do usuário (tais como: nome, data de nascimento, entre outros) que serão posteriormente encaminhados por e-mail para o usuário. |
| 1. O APP necessita manter usuário de sistema. | Crítico | Manter usuários do APP na base de dados. | N/A | Permitir incluir, consultar, alterar e inativar usuários de sistema na base de dados. |
| 1. O APP necessita consultar usuários de sistema. | Útil | Recuperar as informações dos usuários de sistema ativos ou inativos cadastrados na base de dados. | N/A | Permitir consultar as informações de usuários  ativos ou inativos cadastrados na base de dados. |
| 1. O CLIENTE necessita consultar os acessos aos sistemas. | Útil | Recuperar o quantitativo de acessos realizados aos sistemas por meio de URLs. | N/A | Permitir consultar as informações de quantitativo de acessos aos sistemas. |
| 1. O CLIENTE necessita manter perfis. | Crítico | Manter os perfis na base de dados. | N/A | Permitir incluir, consultar, alterar e inativar perfis nos sistemas. |
| 1. O CLIENTE necessita atribuir perfis aos usuários. | Crítico | Garantir a vinculação dos perfis aos usuários do APP | N/A | Permitir vincular os perfis aos usuários de sistemas. |
| 1. O CLIENTE necessita manter o APP | Crítico | Manter o aplicativo na base de dados. | N/A | Permitir incluir, consultar, alterar e inativar o aplicativo. |
| 1. O CLIENTE necessita manter funções de sistemas. | Crítico | Manter funções de sistemas na base de dados. | N/A | Permitir incluir, consultar, alterar e inativar as funções do APP |
| 1. O CLIENTE necessita manter permissões de segurança. | Crítico | Manter permissões de segurança na base de dados. | N/A | Permitir incluir, consultar, alterar e inativar as permissões de segurança. |
| 1. O CLIENTE necessita associar permissões de segurança aos perfis. | Crítico | Garantir a vinculação das permissões de segurança aos perfis. | N/A | Permitir a vincular as permissões de segurança aos perfis. |
| 1. O CLIENTE necessita manter criptografia. | Crítico | Garantir a segurança de dados trafegados. | N/A | Permite a inclusão e renovação de chaves criptográficas no sistema. |
| 1. O CLIENTE necessita analisar solicitação de acesso. | Importante | Garantir que sejam concedidas as permissões de acesso indispensáveis a cada usuário, de acordo com a necessidade. | N/A | Permite a recusa ou a aprovação de uma solicitação de acesso. |
| 1. O CLIENTE necessita consultar as operações realizadas pelo usuário. | Crítico | Apresentar o log das informações que foram incluídas, consultadas, alteradas ou removidas na base de dados. | N/A | Permitir consultar o log de auditoria das operações de inclusão, consulta, alteração e exclusão de informações na base de dados dos sistemas. |
| 1. O CLIENTE necessita transferir os arquivos de logs de auditoria, salvos localmente, para a base de dados externa. | Crítico | Armazenar os arquivos de logs de auditoria, salvos localmente, para a base externa. | N/A | Permitir recuperar o arquivo de log de auditoria, salvo localmente, e armazená-lo na base externa. |
| 1. O CLIENTE necessita apresentar notificação de solicitação de acesso. | Importante | Garantir que as notificações de solicitação de acesso sejam apresentadas no sistema. | N/A | Permitir que as notificações de solicitação de acesso sejam apresentadas no sistema. |
| 1. O CLIENTE necessita descartar logs de auditoria fisicamente. | Importante | Garantir que logs de auditoria possam ser excluídos fisicamente. | N/A | Permitir que os logs de auditora, possam ser excluídos fisicamente. |
| 1. O CLIENTE necessita notificar pendências de solicitação de acesso ao administrador do sistema. | Importante | Garantir que as pendências identificadas na solicitação do acesso sejam notificadas. | N/A | Permite notificar as pendências identificadas na solicitação de acesso ao sistema. |
| 1. O CLIENTE necessita criptografar e descriptografar textos e arquivos no sistema. | Importante | Garantir que textos e arquivos sejam criptografados e descriptografados no sistema. | N/A | Permitir criptografar e descriptografar textos e arquivos no sistema. |
| 1. O CLIENTE necessita que usuários possam assumir representação no sistema. | Importante | Garantir que os usuários logados possam representar outros usuários no sistema. | N/A | Permitir que os usuários logados que possam representar outros usuários no sistema. |
| 1. O CLIENTE necessita manter objeto de segurança. | Crítico | Manter os objetos de segurança nos sistemas | N/A | Permitir incluir, consultar, alterar e inativar os objetos de segurança nos sistemas. |
| 1. O CLIENTE necessita manter classe de segurança | Crítico | Manter classes de segurança nos sistemas. | N/A | Permitir incluir, consultar, alterar e inativar as classes de segurança. |
| 1. O CLIENTE necessita associar classe de segurança ao perfil. | Crítico | Garantir a vinculação das classes de segurança aos perfis. | N/A | Permitir a vinculação das classes de segurança aos perfis. |
| 1. O CLIENTE necessita associar classe de segurança ao objeto de segurança. | Crítico | Garantir a vinculação das classes de segurança aos objetos de segurança. | N/A | Permitir a vinculação das classes de segurança aos objetos de segurança. |
| 1. O CLIENTE necessita associar funções de sistema à permissão de segurança. | Crítico | Garantir a vinculação das funções de sistema à permissão de segurança. | N/A | Permitir a vinculação das funções de sistema à permissão de segurança. |
| 1. O CLIENTE necessita manter representação. | Importante | Manter as representações de um usuário para outro no sistema. | N/A | Permitir a inclusão, alteração, remoção, inativação e ativação de representações. |
| 1. O CLIENTE necessita consultar representação. | Importante | Realizar consultas de todas as representações existentes no sistema. | N/A | Permitir a consulta das representações cadastradas na base. |
| 1. O CLIENTE necessita manter contexto de função. | Crítico | Manter os Contextos de Função do sistema | N/A | Permitir a Inclusão, Alteração, Ativação e Inativação dos Contextos de Função. |
| 1. O CLIENTE necessita associar usuários ao perfil. | Crítico | Garantir a vinculação dos perfis a permissão de segurança. | N/A | Permitir a vinculação  Permitir a vincular as permissões de segurança aos perfis. |
| 1. O CLIENTE necessita solicitar acesso. | Importante | Garantir que o usuário possa solicitar acesso a outros sistemas | N/A | Permitir a solicitação de acesso de usuário cadastrado na base a outros sistemas. |
| 1. O CLIENTE necessita manter página inicial. | Importante | Manter as principais funcionalidades a serem acessadas pelo usuário de acordo com suas permissões. | N/A | Permite a recuperação das informações dos módulos, das principais funcionalidades e dos sistemas para o qual o usuário possui permissão de acesso |
| 1. O CLIENTE necessita de configurar perfil. | Importante | Garantir que o usuário autenticado, possa gerenciar suas informações | N/A | Permite a recuperação das informações pessoais, a alteração da imagem do usuário e o gerenciamento, alteração, remoção, exclusão e inclusão de uma representação, além do acompanhamento das solicitações de acesso. |
| 1. O CLIENTE necessita manter ambiente de sistemas. | Crítico | Manter os ambientes dos sistemas. | N/A | Permite a inclusão, alteração, remoção, ativação e suspenção, direta ou por período. |

# Visão Geral do Produto

## Perspectiva do Produto

O sistema SSA – Sistema de Segurança de Aplicações tem como objetivo possibilitar aos usuários previamente cadastrados a autenticação, a autorização e a auditoria das ações dos usuários nos sistemas. Trata-se de um sistema autossuficiente que deve fornecer toda a estrutura de controle de acesso aos outros sistemas.

## Resumo das Capacidades do Produto

|  |  |
| --- | --- |
| **Benefícios para o Cliente** | **Recursos do Sistema** |
| Acesso único aos sistemas. | A partir da autenticação, é possível que os usuários tenham acesso aos sistemas para os quais possuam permissão. |
| Garantir a segurança dos sistemas. | A segurança será garantida através da autenticação de usuários, das restrições ao acesso das funcionalidades dos sistemas e do monitoramento das ações realizadas nos sistemas. |

# Características do Produto

## Característica 1 – Recuperar usuário e senha [NEC1]

O sistema deve recuperar usuário e senha previamente cadastrados.

## Característica 2 – Verificar usuário ativo [NEC1]

O sistema deve verificar se o usuário possui a situação ativa.

## Característica 3 – Verificar usuário temporário válido [NEC1]

O sistema deve verificar se o usuário temporário possui tempo de acesso válido.

## Característica 4 – Conceder acesso aos sistemas a partir de uma única autenticação [NEC1]

O sistema deve conceder ao usuário, a partir de uma única autenticação, o acesso às aplicações para as quais possua permissão.

## Característica 5 – Validar certificados digitais [NEC1]

O sistema deve validar Certificados Digitais por meio de verificação de *tokens*.

## Característica 6 – Suporte à Federação [NEC1]

O sistema deve oferecer suporte nativo à federação.

## Característica 7 – Redefinição de senha por e-mail [NEC2]

O sistema deve enviar para o e-mail do usuário um conjunto de informações pré-definidas para a redefinição da senha.

## Característica 8 – Redefinição de senha por palavras-chaves [NEC2]

O sistema deve redefinir a senha do usuário por meio de palavras-chaves e questionários.

## Característica 9 – Incluir usuário de sistema [NEC3]

O sistema deve permitir a inclusão de usuários de sistemas na base de dados.

## Característica 10 – Consultar usuário de sistema [NEC3]

O sistema deve permitir a consulta de usuários de sistemas na base de dados.

## Característica 11 – Alterar usuário de sistema [NEC3]

O sistema deve permitir a alteração de usuários de sistemas na base de dados.

## Característica 12 – Inativar usuário de sistema [NEC3]

O sistema deve permitir a inativação de usuários de sistemas na base de dados.

## Característica 13 – Incluir usuário temporário [NEC4]

O sistema deve permitir a inclusão de usuários temporários na base de dados.

## Característica 14 – Consultar usuário temporário [NEC4]

O sistema deve permitir a consulta de usuários temporários na base de dados.

## Característica 15 – Alterar usuário temporário [NEC4]

O sistema deve permitir a alteração de usuários temporários na base de dados.

## Característica 16 – Alterar tempo de acesso de usuário temporário [NEC4]

O sistema deve permitir a alteração do tempo de acesso de usuários temporários na base de dados.

## Característica 17 – Inativar usuário temporário [NEC4]

O sistema deve permitir a inativação de usuários temporários na base de dados.

## Característica 18 – Inativar usuário temporário com tempo de acesso expirado [NEC4]

O sistema deve permitir a inativação de usuários temporários com tempo de acesso expirado na base de dados.

## Característica 19 – Apresentar gráfico de consulta de usuários de sistema [NEC5]

O sistema deve permitir a apresentação do gráfico com consulta de usuários de sistema.

## Característica 20 – Apresentar gráfico da consulta de acessos aos sistemas [NEC6]

O sistema deve permitir a apresentação do gráfico com a consulta de acessos aos sistemas.

## Característica 21 – Incluir perfil [NEC7]

O sistema deve permitir a inclusão de perfis na base de dados.

## Característica 22 – Consultar perfil [NEC7]

O sistema deve permitir a consulta de perfis na base de dados.

## Característica 23 – Alterar perfil [NEC7]

O sistema deve permitir a alteração de perfis na base de dados.

## Característica 24 – Inativar perfil [NEC7]

O sistema deve permitir a inativação de perfis na base de dados.

## Característica 25 – Apresentar perfis [NEC8, NEC12, NEC27]

O sistema deve apresentar todos os perfis do sistema cadastrados na base de dados.

## Característica 26 – Apresentar usuários [NEC8]

O sistema deve apresentar todos os usuários do sistema cadastrados na base de dados.

## Característica 27 – Incluir sistemas aplicativos [NEC9]

O sistema deve permitir a inclusão de sistemas aplicativos na base de dados.

## Característica 28 – Consultar sistemas aplicativos [NEC9]

O sistema deve permitir a consulta de sistemas aplicativos na base de dados.

## Característica 29 – Alterar sistemas aplicativos [NEC9]

O sistema deve permitir a alteração de sistemas aplicativos na base de dados.

## Característica 30 – Inativar sistemas aplicativos [NEC9]

O sistema deve permitir a inativação de sistemas aplicativos na base de dados.

## Característica 31 – Incluir funções de sistemas [NEC10]

O sistema deve permitir a inclusão de funções de sistemas na base de dados.

## Característica 32 – Consultar funções de sistemas [NEC10]

O sistema deve permitir a consulta de funções de sistemas na base de dados.

## Característica 33 – Alterar funções de sistemas [NEC10]

O sistema deve permitir a alteração de funções de sistemas na base de dados.

## Característica 34 – Inativar funções de sistemas [NEC10]

O sistema deve permitir a inativação de funções de sistemas na base de dados.

## Característica 35 – Incluir permissões de segurança [NEC11]

O sistema deve permitir a inclusão de permissões de segurança na base de dados.

## Característica 36 – Consultar permissões de segurança [NEC11]

O sistema deve permitir a consulta de permissões de segurança na base de dados.

## Característica 37 – Alterar permissões de segurança [NEC11]

O sistema deve permitir a alteração de permissões de segurança na base de dados.

## Característica 38 – Inativar permissões de segurança [NEC11]

O sistema deve permitir a inativação de permissões de segurança na base de dados.

## Característica 39 – Apresentar permissões de segurança [NEC12]

O sistema deve apresentar todas as permissões de segurança do sistema cadastradas na base de dados.

## Característica 40 – Associar permissões de segurança à função de sistema [NEC12]

O sistema deve permitir a vinculação das permissões de segurança às funções sistemas.

## Característica 41 – Associar permissões de segurança aos sistemas [NEC12]

O sistema deve permitir a vinculação das permissões de segurança aos sistemas.

## Característica 42 – Ativar usuário de sistema [NEC3]

O sistema deve permitir a ativação de usuários de sistemas na base de dados.

## Característica 43– Recuperar usuário e senha [NEC1]

O sistema deve recuperar usuário e senha previamente cadastrados.

## Característica 44 – Consultar log de auditoria dos acessos realizados via navegadores [NEC14]

O sistema deve permitir a consulta de logs de auditoria das operações dos acessos realizados ao sistema por meio de navegadores web.

## Característica 45 – Consultar acesso aos sistemas [NEC5, NEC6]

O sistema deve permitir consultar os acessos realizados nos sistemas.

## Característica 46 – Consultar chaves criptográficas [NEC13]

O sistema deve permitir a consulta de chaves criptográficas por sistema.

## Característica 47 – Enviar log de auditoria das operações negociais e serviços [NEC19]

O sistema deve permitir o envio para registro (armazenamento) de logs de auditoria das ações realizadas nas funcionalidades negociais ou nos serviços dos sistemas, independente do sucesso da operação.

## Característica 48 – Consultar log de auditoria das operações negociais e serviços [NEC16]

O sistema deve permitir a consulta de logs de auditoria das ações realizadas nas funcionalidades negociais ou nos serviços dos sistemas.

## Característica 49 – Consultar acesso aos usuários [NEC5, NEC6]

O sistema deve permitir consultar os acessos aos usuários, realizados no sistema.

## Característica 50 – Incluir chave criptográfica [NEC13]

O sistema deve permitir a inclusão de chaves criptográficas por sistema.

## Característica 51 – Renovar chave criptográfica [NEC13]

O sistema deve permitir a renovação de chaves criptográficas por sistema.

## Característica 52 – Consultar log de auditoria de operações [NEC18]

O sistema deve permitir a consulta de logs de auditoria das operações de inclusão, consulta, alteração e exclusão realizadas nos sistemas.

## Característica 53 – Consultar acesso aos contextos de funções [NEC5, NEC6]

O sistema deve permitir consultar os acessos aos contextos de função, realizados no sistema.

## Característica 54 – Obter logs de auditoria de operações de acesso via navegadores [NEC19]

O sistema deve permitir a obtenção de logs de auditoria, salvos localmente, dos acessos realizados ao sistema por meio de navegadores web enviados para armazenamento.

## Característica 55 – Armazenar logs de auditoria de operações de acesso via navegadores [NEC19]

O sistema deve permitir o armazenamento de logs de auditoria, salvos localmente, dos acessos realizados ao sistema por meio de navegadores web.

## Característica 56 – Obter logs de auditoria das operações negociais e serviços [NEC19]

O sistema deve permitir a obtenção de logs de auditoria, salvos localmente, das ações realizadas nas funcionalidades negociais ou nos serviços dos sistemas enviadas para armazenamento.

## Característica 57 – Armazenar logs de auditoria das operações negociais e serviços [NEC19]

O sistema deve permitir o armazenamento de logs de auditoria, salvos localmente, das ações realizadas nas funcionalidades negociais ou nos serviços dos sistemas.

## Característica 58 – Obter logs de auditoria das operações de persistência [NEC19]

O sistema deve permitir a obtenção de logs de auditoria, salvos localmente, das operações de inclusão, consulta, alteração e exclusão de informações na base de dados dos sistemas enviadas para armazenamento.

## Característica 59 – Armazenar logs de auditoria das operações de persistência [NEC19]

O sistema deve permitir o armazenamento de logs de auditoria, salvos localmente, das operações de inclusão, consulta, alteração e exclusão de informações na base de dados dos sistemas.

## Característica 60 – Apresentar notificação de solicitação de acesso ao administrador [NEC20]

O sistema deve permitir a apresentação das notificações de solicitação de acesso enviadas ao administrador do sistema.

## Característica 61 – Apresentar notificação de acesso ao usuário solicitante [NEC20]

O sistema deve permitir a apresentação das notificações de solicitação de acesso respondidas pelo administrador ao usuário solicitante.

## Característica 62 – Consultar logs de auditoria para descarte [NEC21]

O sistema deve permitir a consulta dos logs de auditoria para descarte.

## Característica 63 – Descartar logs de auditoria [NEC21]

O sistema deve permitir a exclusão logica dos logs de auditoria fisicamente.

## Característica 64 – Verificar quantidade de notificações pendentes [NEC22]

O sistema deve permitir a verificação da quantidade de notificações de solicitação de acesso pendentes.

## Característica 65 – Apresentar notificação pendente [NEC22]

O sistema deve permitir a apresentação da notificação de pendência após sete dias do recebimento da solicitação de acesso.

## Característica 66 – Criptografar textos e arquivos [NEC23]

O sistema deve permitir a criptografia de textos e arquivos claros, por meio de chave criptográfica, no sistema.

## Característica 67 – Descriptografar textos e arquivos [NEC23]

O sistema deve permitir a descriptografia de textos e arquivos cifrados, por meio de chave criptográfica, no sistema.

## Característica 68 – Recuperar usuários representados [NEC24]

O sistema deve permitir a listagem dos usuários representados pelo usuário *logado*.

## Característica 69 – Representar usuário no sistema [NEC24]

O sistema deve permitir que o usuário *logado* possa representar outro usuário no sistema.

## Característica 70 – Apresentar imagem de perfil do usuário representado [NEC24]

O sistema deve permitir a apresentação da imagem do perfil de cada usuário representado listado.

## Característica 71 – Apresentar funcionalidades do usuário representado [NEC24]

O sistema deve permitir a apresentação das funcionalidades que o usuário representado possui permissão de acesso.

## Característica 72 – Assumir representação [NEC24]

O sistema deve permitir a inclusão da representação na base de dados.

## Característica 73 – Armazenar situação da notificação [NEC20]

O sistema deve permitir o armazenamento da situação da notificação na base de dados.

## Característica 74 – Gerar chave criptográfica para o sistema [NEC23]

O sistema deve permitir a geração de chave criptográfica para o sistema.

## Característica 75 – Consultar acesso às funções de sistema [NEC5, NEC6]

O sistema deve permitir consultar os acessos às funções de sistema, realizados no sistema.

## Característica 76 – Incluir objeto de segurança [NEC25]

O sistema deve permitir a inclusão de objetos de segurança nos sistemas.

## Característica 77 – Consulta objeto de segurança [NEC25]

O sistema deve permitir a consulta de objetos de segurança nos sistemas.

## Característica 78 – Alterar objeto de segurança [NEC25]

O sistema deve permitir a alteração de objetos de segurança nos sistemas.

## Característica 79 – Remover objeto de segurança [NEC25]

O sistema deve permitir a remoção de objetos de segurança nos sistemas.

## Característica 80 – Incluir classe de segurança [NEC26]

O sistema deve permitir a inclusão de classes de segurança nos sistemas.

## Característica 81 – Consulta classes de segurança [NEC26]

O sistema deve permitir a consulta de classes de segurança nos sistemas.

## Característica 82 – Alterar classe de segurança [NEC26]

O sistema deve permitir a alteração de classes de segurança nos sistemas.

## Característica 83 – Remover classe de segurança [NEC26]

O sistema deve permitir a remoção de classes de segurança nos sistemas.

## Característica 84 – Apresentar classe de segurança [NEC27, NEC28]

O sistema deve apresentar todos as classes de segurança do sistema cadastradas na base de dados.

## Característica 85 – Apresentar objeto de segurança [NEC28]

O sistema deve apresentar todos aos objetos de segurança do sistema cadastrados na base de dados.

## Característica 86 – Apresentar funções de sistema [NEC29]

O sistema deve apresentar todos as funções de sistema cadastradas na base de dados.

## Característica 87 – Apresentar permissão de segurança [NEC29]

O sistema deve apresentar todos as permissões de segurança do sistema cadastradas na base de dados.

## Característica 88 – Incluir representação [NEC30, NEC36]

O sistema deve permitir a inclusão de representações no sistema.

## Característica 89 – Alterar representação [NEC30, NEC36]

O sistema deve permitir a alteração de representações no sistema.

## Característica 90 – Remover representação [NEC30, NEC36]

O sistema deve permitir a remoção de representações no sistema.

## Característica 91 – Apresentar representação [NEC30]

O sistema deve permitir a apresentação das representações do usuário no sistema.

## Característica 92 – Inativar representação [NEC30]

O sistema deve permitir a inativação de representações no sistema.

## Característica 93 – Ativar representação [NEC30]

O sistema deve permitir a ativação de representações no sistema.

## Característica 94 – Consultar representações [NEC31]

O sistema deve permitir a consulta de todas as representações existentes na base de dados.

## Característica 95 – Incluir contexto de função [NEC32]

O sistema deve permitir a inclusão de todas de um contexto de função.

## Característica 96 – Consultar contexto de função [NEC32]

O sistema deve permitir a consulta de todos os contextos de função existentes na base de dados.

## Característica 97 – Alterar contexto de função [NEC32]

O sistema deve permitir a alteração de um contexto de função existente na base de dados.

## Característica 98 – Inativar contexto de função [NEC32]

O sistema deve permitir a inativação de um contexto de função.

## Característica 99 – Ativar contexto de função [NEC32]

O sistema deve permitir ativação de um contexto de função

## Característica 100 – Associar usuários ao perfil [NEC33]

O sistema deve permitir a vinculação de usuários ao perfil.

## Característica 101 – Solicitar acesso [NEC34]

O sistema deve permitir encaminhar uma solicitação de acesso a um determinado sistema cadastrado na base de dados.

## Característica 102 –Apresentar página inicial [NEC35]

O sistema deve apresentar as informações existentes na base de dados de acordo com cada usuário.

## Característica 103 – Visualizar informações pessoais do usuário [NEC36]

O sistema deve permitir a visualização das informações pessoais do usuário.

## Característica 104 – Visualizar solicitações de acesso [NEC36]

O sistema deve permitir a visualização das solicitações de acesso realizadas por um usuário.

## Característica 105 – Remover notificação [NEC22]

O sistema deve permitir a remoção da notificação de solicitação de acesso já analisada.

## Característica 106 – Limpar visualização das notificações [NEC22]

O sistema deve permitir limpar a exibição das notificações que foram visualizadas a mais de 10 dias.

## Característica 107 – Inativar representação [NEC30, NEC36]

O sistema deve permitir a inativação de representações.

## Característica 108 – Ativar representação [NEC30, NEC36]

O sistema deve permitir a ativação de representações.

## Característica 109 – Gerar procuração para representação [NEC30]

O sistema deve gerar um documento para formalizar as representações definidas no sistema.

## Característica 110 – Incluir ambiente [NEC37]

O sistema deve permitir a inclusão de ambientes para cada sistema cadastrado.

## Característica 111 – Alterar ambiente [NEC37]

O sistema deve a alteração de um ambiente.

## Característica 112 – Remover ambiente [NEC37]

O sistema deve permitir a remoção de ambientes.

## Característica 113 – Suspender ambiente [NEC37]

O sistema deve permitir a suspensão por ambiente.

## Característica 114 – Suspender ambiente por período [NEC37]

O sistema deve permitir o agendamento de uma suspensão por ambiente.

## Característica 115 – Ativar ambiente [NEC37]

O sistema deve permitir a ativação de ambiente.

## Característica 116 – Aprovar solicitação de acesso [NEC17]

O sistema deve permitir a aprovação de uma solicitação de acesso.

## Característica 117 – Recusar solicitação de acesso [NEC17]

O sistema deve permitir a recusa de uma solicitação de acesso.

## Característica 118 – Configurar níveis de auditoria [NEC15]

O sistema deve permitir a configuração das necessidades de auditoria.

# Interface com Outros Sistemas

|  |  |  |
| --- | --- | --- |
| **Sistema** | **Descrição** | **Tipo da Integração** |
| Sistema de recursos humanos. | Sistema destinado ao controle de pessoal do órgão. | Tipo 1  Tipo 3  Tipo 4 |
| Sistema de cadastro de instituições. | Sistema destinado ao controle de instituições que relacionam com o órgão. | Tipo 1  Tipo 3  Tipo 4 |
| Sistema de serviços de diretório distribuído – LDAP. | Sistema destinado ao cadastro de usuários de sistemas do órgão. | Tipo 1  Tipo 4 |

**Sistema A**: Sistema objeto desse documento de escopo preliminar.

**Sistema B**: Sistema a se integrar com o sistema A

Tipo 1: Sistema A consulta dados/informações no sistema B;

Tipo 2: Sistema A atualiza dados/informações no sistema B;

Tipo 3: Sistema A gera dados/informações para processamento no sistema B;

Tipo 4: Sistema A processa dados/informações gerado por B.

# Restrições Impostas

## Econômicas

Não se aplica.

## Tecnologia

As restrições impostas por tecnologia estão descritas no Documento de Arquitetura de Software.

## Sistemas

As restrições impostas por sistemas estão descritas no Documento de Arquitetura de Software.

## Ambiente

As restrições impostas por ambiente estão descritas no Documento de Arquitetura de Software.

## Prazos e Custos

As restrições impostas por prazos e custos estão descritas no Plano de Projetos.

# Precedência e Prioridade

O sistema SSA – Sistema de Segurança de Aplicações é composto pelos módulos de Autenticação, Autorização e Auditoria.

No primeiro módulo a ser executado, o módulo de Autenticação, os usuários podem ser identificados por meio de *login* único no sistema SSA. Após autenticação, são estabelecidas as permissões do usuário para executar determinadas operações no sistema, através do módulo de Autorização. Por fim, o módulo de Auditoria monitora as ações realizadas pelo usuário no sistema.

# Requisitos de Documentação

## Manual do Usuário

Será desenvolvido e disponibilizado pela CTIS, em meio magnético, ao final do projeto, o manual do usuário contendo o conjunto de orientações para o uso e navegação eficaz da aplicação como:

* Objetivos;
* Abrangência do sistema;
* Descrição do sistema;
* Ativação do sistema;
* Utilização do sistema;
* Emissão de relatórios;
* Layouts dos relatórios.

## Ajuda On-Line

Não se aplica.

## Guias de Instalação, de Configuração e arquivo Leia-me

Não se aplica.

# Anexos

Não se aplica.

# Referências

* Plano de Gerenciamento de Requisitos – SSA\_PlanoGerenciamentoRequisitos.docx;
* Plano de Projetos – SSA\_PlanoProjeto.docx;
* Documento de Arquitetura de Software – SSA\_DocumentoArquiteturaSoftware.docx.

# Aprovações

|  |  |  |
| --- | --- | --- |
| **Aprovações** | | |
| **Participante** | **Assinatura** | **Data** |
|  |  |  |
|  |  |  |