



SGAVSEC

Manual do Sistema de Gestão AVSEC
SGAVSEC

1 INTRODUÇÃO

O Sistema de Gestão AVSEC (SGAVSEC) é uma ferramenta corporativa desenvolvida pelo Departamento de Controle do Espaço Aéreo (DECEA) com a finalidade de apoiar a gestão das atividades de segurança da aviação civil contra atos de interferência ilícita no âmbito do Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB).

Inserido no contexto do Sistema de Gerenciamento da Segurança AVSEC (SeMS), o SGAVSEC constitui um instrumento essencial para o fortalecimento da governança, da supervisão baseada em risco e da cultura de segurança da aviação, permitindo a integração de processos, padronização de informações e rastreabilidade das ações realizadas.

O sistema foi estruturado de forma modular, contemplando funcionalidades que abrangem o registro e tratamento de relatos de segurança (RELSEC), o gerenciamento de riscos, o controle de qualidade, a promoção da segurança AVSEC, a geração de indicadores estratégicos e o suporte às auditorias internacionais conduzidas pela Organização da Aviação Civil Internacional (OACI), especialmente no âmbito do Programa Universal de Auditoria de Segurança da Aviação Civil – Abordagem de Monitoramento Contínuo (USAP-CMA).

Além disso, o SGAVSEC possibilita a centralização das informações relacionadas à segurança da aviação no SISCEAB, promovendo o compartilhamento de boas práticas entre os Provedores de Serviços de Navegação Aérea (PSNA) e contribuindo para a melhoria contínua dos processos e para o aumento da maturidade institucional na gestão da segurança AVSEC.

O acesso ao sistema é realizado por usuários devidamente credenciados, com níveis de permissão definidos conforme suas atribuições, sendo também disponibilizado, de forma controlada, o registro ostensivo de relatos de segurança por usuários externos, ampliando a capacidade de identificação de vulnerabilidades e ocorrências.

Este manual tem como finalidade orientar os usuários quanto à utilização do SGAVSEC, descrevendo suas funcionalidades, fluxos operacionais e responsabilidades associadas, de modo a assegurar o uso adequado do sistema e a qualidade das informações registradas.

2 GESTÃO DE USUÁRIOS

2.1 Cadastro de Usuários

O cadastro de usuários no SGAVSEC é realizado pelos gerentes do sistema, conforme os níveis de responsabilidade estabelecidos.

O Gerente Nacional possui autonomia para cadastrar usuários vinculados à Assessoria de Segurança da Aviação Civil no Controle do Espaço Aéreo (AVSECCEA), bem como os gerentes dos órgãos regionais do DECEA.

Os Gerentes Regionais, por sua vez, podem cadastrar os agentes de suas respectivas assessorias regionais e os Gerentes Locais das unidades sob sua jurisdição.

Os Gerentes Locais são responsáveis pelo cadastro dos usuários vinculados aos agentes locais de suas unidades.

Para criar usuários, o gerente deverá acessar a aba “Usuários”, selecionar a opção “Adicionar”, escolher o elo do SISCEAB correspondente e preencher os campos com os dados do novo usuário.

O SGAVSEC possui dois tipos de modo de acesso: “Gerenciamento”, com possibilidade de elaborar RELSEC, realizar gerenciamento do risco, cadastrar usuários (no caso perfil de Gerentes). E modo “Observador”, onde usuário terá perfil apenas para visualizar RELSEC e acompanhar gerenciamento de risco dos elos em que estiver cadastrado.

Há também a possibilidade de cadastrar usuário em diversos elos (“Elos Locais Adicionais”), para os casos de usuários que gerenciam mais de um elo local. Caso este usuário gerencie elos em diferentes regionais, as informações para cadastro devem ser enviadas para a AVSECCEA (avsec@decea.mil.br).

Informações do Usuário

Lembrete!
Será enviada por e-mail uma senha provisória ao novo usuário.

Elo SISCEAB *

Escolha um Elo

Tipo Agente *

Escolha o perfil

Selecione primeiramente um Elo SISCEAB

Modo de acesso *

Gerenciamento

Elos Locais Adicionais
Disponível apenas para perfis de Gerente Local.

Nome *

Nome completo

E-mail *

E-mail

Posto/Graduação/Civil *

Escolha uma opção

Telefone *

(00) 00000-0000

Salvar

AVSECCEA – Assessoria de Segurança da Aviação Civil no Controle do Espaço Aéreo (SDAD/DECEA).
Recomendamos o uso do Google Chrome ou Microsoft Edge. Versão: 1.23

Figura 1: Cadastro de usuário do SGAVSEC

2.2 Primeiro acesso ao sistema

Após o cadastro, o sistema encaminha ao usuário um e-mail contendo instruções para definição de senha.

Por segurança, o *link* contido no e-mail de cadastro inicial do sistema tem a duração de 96 horas. Após esse período, o gerente deve utilizar a aba de gestão de usuários para enviar novo link para a definição de senha. Já o link de reset de senha tem a validade de 24 horas.

Bem-vindo ao SGAVSEC!

Para continuar, clique no botão abaixo e defina sua senha inicial:

Definir Senha

Caso o botão acima não funcione, copie e cole o link abaixo no seu navegador:

<https://sgavsec.decea.mil.br/users/set-password-confirm/MjAy/d61zup-f754f2e8e702104e279a218b178466ef/>

Seu nome de usuário (e-mail): joaocpb@gmail.com

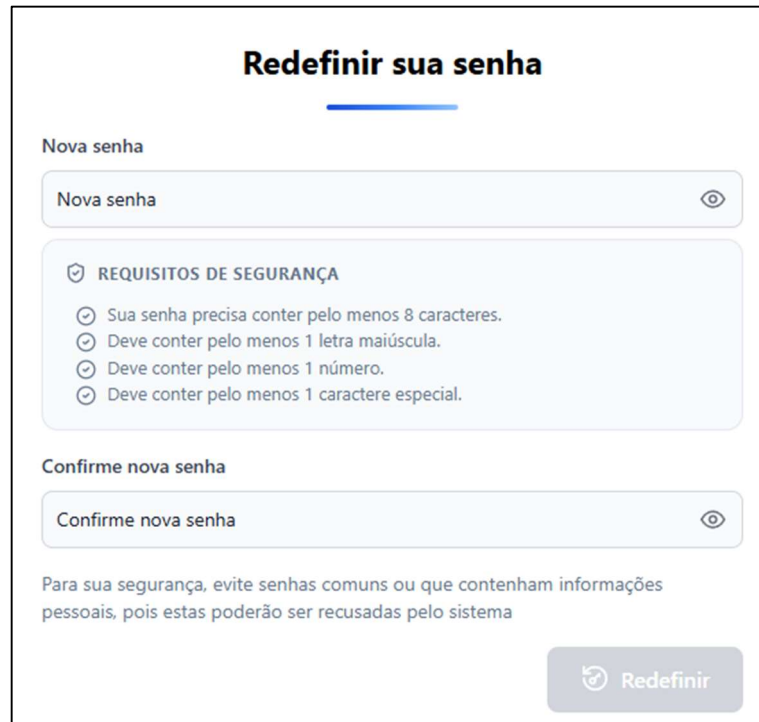
Este link expira em **96 horas** por motivos de segurança.

Figura 2: E-mail recebido pelo usuário para a definição de senha

Conforme ilustrado na Figura 2, para acessar o sistema, o usuário deve clicar no botão “Definir Senha” ou, alternativamente, utilizar o link disponibilizado, podendo acessá-lo diretamente ou copiá-lo e

colá-lo no navegador.

A Figura 3 apresenta a tela de criação de senha para acesso ao sistema. A senha deve atender aos requisitos de segurança estabelecidos, conforme indicado na própria tela.



Redefinir sua senha

Nova senha

Nova senha

REQUISITOS DE SEGURANÇA

- ✓ Sua senha precisa conter pelo menos 8 caracteres.
- ✓ Deve conter pelo menos 1 letra maiúscula.
- ✓ Deve conter pelo menos 1 número.
- ✓ Deve conter pelo menos 1 caractere especial.

Confirme nova senha

Confirme nova senha

Para sua segurança, evite senhas comuns ou que contenham informações pessoais, pois estas poderão ser recusadas pelo sistema

 Redefinir

Figura 3: Criação de senha com os requisitos mínimos de segurança

Após a redefinição de senha, o usuário é direcionado à página de login do sistema <https://sgavsec.decea.mil.br>

No campo “Usuário”, deve ser inserido o endereço de e-mail completo cadastrado no sistema.

No campo “Senha”, deve ser informada a senha recém-criada.

No primeiro acesso, o campo “Código de verificação (2FA)” deve ser deixado em branco, uma vez que o processo de ativação da autenticação em dois fatores será solicitado em etapa posterior.

The image shows a login interface titled "Autenticação". It contains three input fields: "Usuário" with the placeholder "nome@dominio.com", "Senha" with masked characters ".....", and "Código de verificação (2FA)" with the value "123456". Below the 2FA field is a note: "Obrigatório se você já ativou. Caso contrário, deixe em branco." There is a checkbox labeled "Lembrar-me" and a link "Esqueceu a senha?". At the bottom is a blue button labeled "Acessar conta".

Autenticação

Usuário
nome@dominio.com

Senha
.....

Código de verificação (2FA)
123456
Obrigatório se você já ativou. Caso contrário, deixe em branco.

☐ Lembrar-me

[Esqueceu a senha?](#)

Acessar conta

Figura 4: Login no SGAVSEC

Após a inserção dos dados de acesso, mantendo o campo “Código de verificação (2FA)” em branco, conforme ilustrado na Figura 4, o usuário será direcionado à etapa de ativação da autenticação em dois fatores, a ser realizada por meio de aplicativo instalado em dispositivo móvel.

Para a realização desta etapa, o usuário deverá instalar, em dispositivo móvel, um aplicativo compatível com autenticação em dois fatores (2FA), como Microsoft Authenticator, Google Authenticator, Authy, entre outros.

Com o aplicativo aberto, deverá ser realizada a vinculação da conta, por meio da leitura do QR Code ou da inserção manual da chave gerada pelo SGAVSEC.

Após a configuração, o aplicativo exibirá um código de verificação temporário, o qual deverá ser inserido no campo “Código de verificação” do sistema para a efetivação da autenticação em dois fatores.

Autenticação em Dois Fatores (Segurança em 2 etapas)

Proteja sua conta escaneando o código abaixo com seu app de autenticação preferido.



APONTE A CÂMERA

1

 Abra o **Google Authenticator** ou similar.

2

 Escaneie o QR Code e digite os **6 dígitos** gerados.

3

 Se a câmera não conseguir ler, cadastre manualmente a chave abaixo no app.

Chave manual do autenticador

Copiar chave

DJZC MP74 BV6C OIWO FNPD KNBX RTD4 N52J

Use esta chave apenas se o QR Code não puder ser lido pelo aplicativo autenticador.

CÓDIGO DE VERIFICAÇÃO

000000

✓ Ativar Segurança

Figura 5: Ativação em dois fatores (2FA)

Na sequência, o usuário deverá ler e aceitar o Termo de Responsabilidade para uso do SGAVSEC. O referido termo poderá ser acessado posteriormente por meio do menu superior do sistema.

DOCUMENTO OFICIAL

Atualizado em 25/02/2026

TERMO DE RESPONSABILIDADE PARA USO DO SISTEMA DE GESTÃO AVSEC (SGAVSEC)

Como usuário do SGAVSEC comprometo-me a:

- Utilizar os serviços de rede da INTRAER e da Internet disponibilizados pelo DECEA somente para apoio às atividades de interesse do COMAER;
- Não compartilhar senhas de acesso ao SGAVSEC, assumindo integral responsabilidade pela sua guarda e sigilo, bem como pelo uso indevido de terceiros;
- Não inserir senhas de acesso em mensagens de e-mail ou qualquer outra forma de comunicação eletrônica;
- Não me ausentar da estação de trabalho sem encerrar a sessão, impedindo o uso indevido de minhas credenciais de acesso por pessoas não autorizadas;
- Não utilizar métodos para obtenção de acessos indevidos às estações de trabalhos, arquivos, conteúdos de internet ou qualquer outro recurso de TI;
- Não armazenar nos recursos de TI sob minha responsabilidade software comercial ou qualquer outro material cujo direito pertença a terceiros (*copyright*), sem que haja um contrato de licenciamento ou outros tipos de licença;
- Notificar o Centro de Operações de Segurança (SOC), do Centro de Gerenciamento Técnico (CGTEC), do Parque de Material de Eletrônica do Rio de Janeiro (PAME-RJ) através do e-mail: _soc.decea@fab.mil.br qualquer comportamento suspeito que possa representar uma ameaça à Segurança da Informação ou um Incidente de Segurança; *atentar para o *underline* antes do e-mail.
- Comunicar com a maior brevidade possível o meu desligamento da organização ou mudança de função para a regularização do acesso ao SGAVSEC.

Ao clicar em **Aceitar e Continuar**, você declara ciência das normas de segurança e autoriza o registro do seu IP e credenciais para fins de auditoria.

Cancelar

Aceitar e Continuar

Figura 6: Termo de Responsabilidade para o uso do SGAVSEC

O sistema permite que os usuários atualizem seus dados cadastrais e realizem o envio da foto de perfil.

Com o objetivo de manter a padronização do banco de dados, a foto de perfil deverá atender aos seguintes critérios: para usuários militares, deve ser utilizada a mesma imagem constante no Sistema de Gerenciamento de Pessoal da Aeronáutica (SIGPES); para usuários civis, deve ser utilizada fotografia no formato 5x7, com enquadramento adequado do rosto.

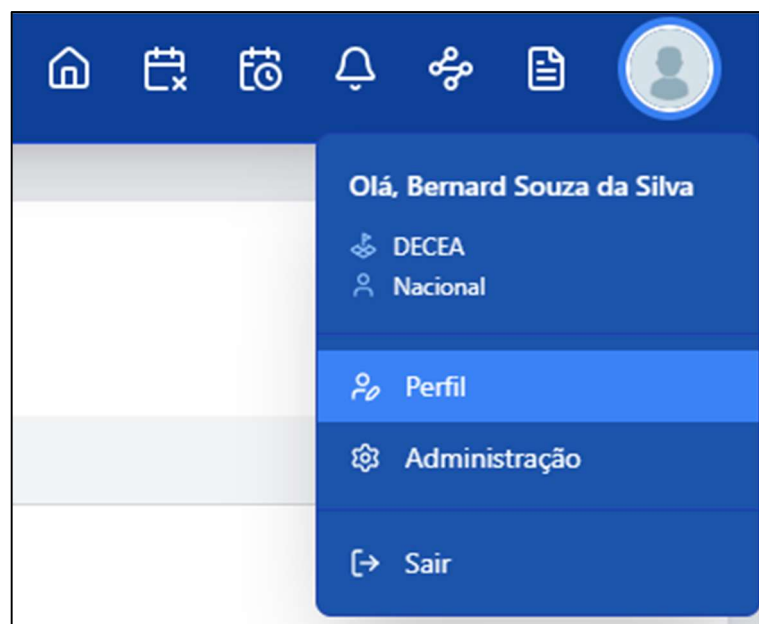


Figura 7: Acesso aos ajustes de perfil de usuário

2.3 Redefinição de senha

Caso o usuário deseje alterar sua senha, deverá acessar a tela de perfil, localizar o campo específico, inserir a senha atual e a nova senha.

Figura 8: Redefinição de senha

2.4 Esqueci a senha

Caso o usuário esqueça a senha, poderá solicitar sua redefinição por meio da funcionalidade disponível na tela de login.

Para isso, deverá acessar a página principal do SGAVSEC, <https://sgavsec.decea.mil.br>, selecionar a opção “Entrar” no canto superior à direita, clicar em “Esqueci a senha” e informar o e-mail cadastrado pelo gerente de sua organização.

Figura 9: Processo de redefinição de senha

Após a solicitação, será encaminhado ao usuário um e-mail contendo instruções para redefinição da senha.

Ressalta-se que o código de autenticação em dois fatores (2FA), configurado no primeiro acesso, permanece válido. Caso o aplicativo autenticador tenha sido desinstalado, a desabilitação do 2FA deverá ser solicitada ao gerente, o qual dispõe da funcionalidade de redefinição de senha e de reset da autenticação em dois fatores (2FA) dos usuários sob sua jurisdição. Para isso, o gerente deverá acessar o menu “Usuários”, localizar o usuário desejado e selecionar a ação correspondente: “Resetar senha” e/ou “Resetar 2FA”.

Figura 10: Redefinição de senha e 2FA pelo gerente

2.5 Desativação e Exclusão de Usuários

A exclusão de usuários no sistema somente é permitida quando não houver registros de interação

a eles associados.

Caso o usuário já tenha realizado ações no SGAVSEC, será admitida apenas a sua desativação, de modo a preservar a integridade e a rastreabilidade das informações registradas.

Em conformidade com o Termo de Responsabilidade de uso do SGAVSEC, os usuários com perfil de gerente são responsáveis pela manutenção da lista de usuários cadastrados, devendo desativar aqueles que não mais pertençam aos setores responsáveis pela atividade AVSEC em suas respectivas organizações.

Para desativar ou excluir um usuário, o gerente deverá acessar o SGAVSEC, realizar o login no sistema, selecionar a aba lateral “Usuários”, localizar o usuário desejado e escolher a opção “Desativar” ou “Excluir”, conforme aplicável.

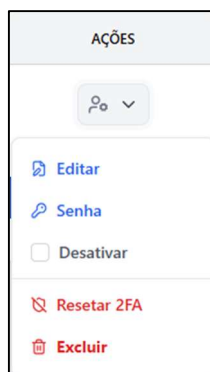


Figura 11: Seleção de desativação e exclusão de usuários

3 RELSEC

De acordo com os regulamentos do DECEA, este relato será utilizado para informação de vulnerabilidades e registro de ocorrências de atos de interferência ilícita (AVSEC), contribuindo para o fortalecimento da segurança da aviação civil. A identificação do autor não é obrigatória; no entanto, caso opte por se identificar, será informado sobre a resolução da situação reportada ao término do processo.

O RELSEC destina-se também para reportar ocorrências de ilícitos e eventos onde ocorreu impacto na Segurança AVSEC e, consequentemente, prejuízo e/ou danos nas operações de controle de tráfego aéreo em um Elo do SISCEAB. Esta ferramenta constitui o principal instrumento de registro de ocorrências AVSEC no SGAVSEC.

3.1 Preenchimento do RELSEC

O registro deve conter:

- a) Data e hora da ocorrência;
- b) Elo do SISCEAB envolvido;
- c) Descrição detalhada da ocorrência;
- d) Assunto;
- e) Localização;
- f) Informações sobre pessoas envolvidas; e
- g) Identificação do relator (opcional).

Recomenda-se inserir o máximo de dados disponíveis, incluindo referências e evidências anexadas (mais detalhes sobre tamanho e tipo de arquivos que podem ser anexados estão no tópico a seguir).

O RELSEC pode ser realizado com usuário logado ou por usuário externo, sem login ou cadastro. E caso o relator se identifique, receberá por e-mail tratamento da ocorrência, se o assunto não for de caráter restrito.

Formulário para registro de RELSEC

De acordo com os regulamentos do DECEA, este relato será utilizado para informação de vulnerabilidades e registro de ocorrências de atos de interferência ilícita (AVSEC), contribuindo para o fortalecimento da segurança da aviação civil. **A identificação do autor não é obrigatória;** no entanto, caso opte por se identificar, será informado sobre a resolução da situação reportada ao término do processo.

Data e hora da ocorrência (Hora local)

Elo SISCEAB

dd/mm/aaaa --:--

Escolha um Elo

Ocorrência

Descreva a ocorrência e, se aplicável, informe as medidas mitigadoras tomadas.

Assunto

Estado

Cidade

Geolocalização

Escolha um assunto

UF

Escolha uma cidade

 latitude, longitude

Para definir o local exato, clique na caixa acima para pesquisar no mapa.

Pessoal envolvido

Descreva os envolvidos

 Arquivos

Nenhum arquivo selecionado

Arquivo(s)

Extensões permitidas: PDF, PNG, JPG, MP4

Máx: 5 MB /arq (até 3 arquivos).

Identificação (Opcional)

Nome

E-mail

Contato

 nome@email.com

 00-00000-0000

Caso queira receber uma cópia desse RELSEC

Enviar

Figura 12: Formulário para registro de RELSEC

3.2 Geolocalização

O sistema permite definir localização do RELSEC por meio de mapa interativo com ferramenta de busca, ajuste de zoom e precisão, incluindo modo satélite, registrando assim maior exatidão do ponto geográfico.

Após identificar o local no mapa, o usuário deve clicar em “Inserir” (canto inferior, à direita), para que o sistema identifique as coordenadas. Automaticamente o Estado e a Cidade serão identificados.

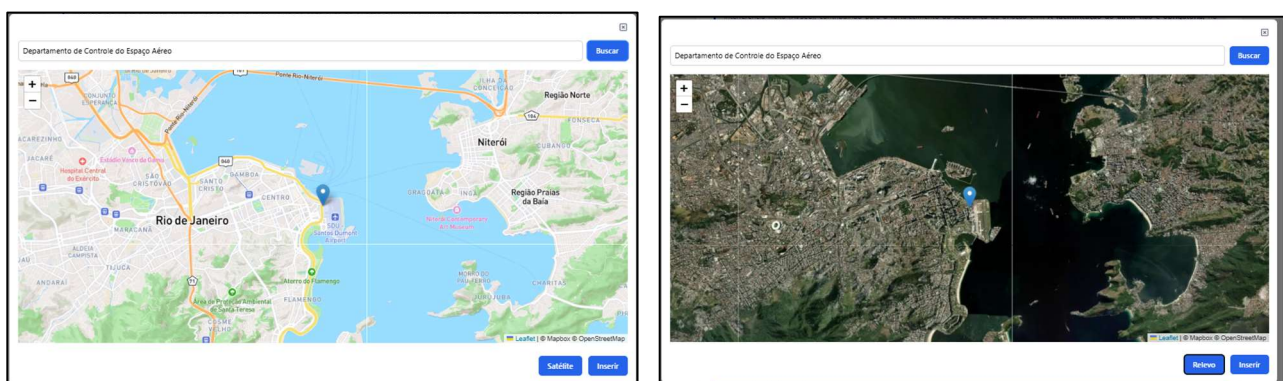


Figura 13: Tela de geolocalização (modo: relevo e satélite)

3.3 Anexos e Evidências

Podem ser documentos, atas, transcrições de livro de ocorrências, imagens ou outros arquivos relevantes. As extensões de arquivos permitidas são: PDF, PNG, JPG, MP4 - contendo no máximo 5MB por arquivo e até três arquivos

