

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



INTELIGÊNCIA

FCA 200-7

CONTROLE DA REDE INFOSEG NO COMAER

2022

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA**



INTELIGÊNCIA

FCA 200-7

CONTROLE DA REDE INFOSEG NO COMAER

2022



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

PORTARIA CIAER Nº 1/DPL, de 08 de MARÇO de 2022.

Aprova a edição do Folheto que dispõe sobre o Controle da Rede INFOSEG no COMAER.

O CHEFE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA, tendo em vista o disposto no Inciso III, do art. 4º do Regulamento do Centro de Inteligência da Aeronáutica, aprovado pela Portaria nº 1.546/GC3, de 3 de outubro de 2018, resolve:

Art. 1º Aprovar a edição do FCA 200-7 “Controle da Rede INFOSEG no COMAER”, que com esta baixa.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Brig Ar RODRIGO GIBIN DUARTE
Chefe do CIAER

(Publicada no BCA nº 052, de 17 de março de 2022)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES	09
1.1 FINALIDADE	09
1.2 ÂMBITO	09
1.3 NOÇÕES FUNDAMENTAIS.....	09
2 PROCESSO DE CADASTRAMENTO	10
2.1 REQUISITOS OBRIGATÓRIOS DAS ORGANIZAÇÕES MILITARES.....	10
2.2 REQUISITOS OBRIGATÓRIOS DOS INDICADOS	10
2.3 PROCEDIMENTOS PARA O CADASTRAMENTO	10
3 PROCEDIMENTOS PARA UTILIZAÇÃO	11
4 NORMAS DE SEGURANÇA	12
4.1 POLÍTICA DE SENHAS	12
5 RESPONSABILIDADES DOS MILITARES CADASTRADOS	13
6 DISPOSIÇÕES FINAIS.....	14
REFERÊNCIAS	15
Anexo A – Modelo de relatório do INFOSEG.....	16
Anexo B – Termo de compromisso de manutenção de sigilo-INFOSEG.....	17

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O presente Folheto dispõe sobre o controle ao Sistema INFOSEG, tendo por finalidade orientar os usuários quanto ao cadastramento, acesso e utilização do Sistema.

1.2 ÂMBITO

A presente legislação tem sua aplicação no âmbito do SINTAER.

1.3 NOÇÕES FUNDAMENTAIS

1.3.1 O Sistema Nacional de Informações de Segurança Pública (INFOSEG) tem por objetivo principal a integração das informações de indivíduos criminalmente identificados, de armas de fogo, de veículos e de condutores, entre todas as Unidades da Federação.

1.3.2 O Sistema é gerenciado pela Secretaria Nacional de Segurança Pública (SENASP), órgão subordinado ao Ministério da Justiça e Segurança Pública (MJSP), e disponibiliza informações de Segurança Pública e Justiça por meio de uma rede privativa em âmbito nacional. Atualmente este sistema também pode ser acessado pela Internet, utilizando um índice onde é possível obter informações básicas de indivíduos. O detalhamento dessas informações é disponibilizado a partir de uma consulta inicial ao índice, diretamente nas bases estaduais de origem, mantendo a autonomia dos estados e de outras bases de Segurança Pública e Justiça em relação às suas informações detalhadas. O Sistema INFOSEG concentra em sua base de dados apenas as informações básicas que apontam para as fontes de dados dos estados.

1.3.3 A plataforma do Sistema também permite a integração de forma rápida e confiável, seguindo todos os padrões de segurança necessários, com outras bases de dados, como é o caso das informações de veículos, condutores, armas e detalhamento de informações de indivíduos nas bases estaduais, disponibilizadas aos usuários do INFOSEG.

1.3.4 A alimentação dos dados na base do INFOSEG é feita por uma solução de atualização em tempo real, onde, à medida que a base de dados do estado sofre uma atualização, é gerado um registro e este é atualizado no Índice Nacional do INFOSEG. Dessa forma a base de dados do Índice Nacional refletirá fielmente a realidade das bases estaduais.

1.3.5 Com o objetivo de seguir as diretrizes do Sistema, a SENASP decidiu por reestruturar o módulo de administração com o objetivo de prover maior facilidade, confiabilidade e segurança nos acessos realizados pelos usuários. Todos os módulos de autenticação, autorização e auditoria foram otimizados para melhor atender os quesitos de segurança necessários em um acesso disponibilizado via Internet.

1.3.6 Visando atualizar os métodos de utilização e controle do Sistema, a SENASP implementou novas formas de cadastramento, agora totalmente via Internet, com um acréscimo de camadas de proteção contra o uso indevido do Sistema, como o número de telefone autenticador. No mesmo sentido, outros dispositivos e controles serão inseridos no projeto, a critério exclusivo do MJSP.

2 PROCESSO DE CADASTRAMENTO

2.1 REQUISITOS OBRIGATÓRIOS DAS ORGANIZAÇÕES MILITARES

2.1.1 O acesso à Rede INFOSEG será concedido às OM pertencentes ao SINTAER de acordo com o seguinte critério:

- a) Estar categorizado como Elo Tipo “S” e “E”;
- b) Estar categorizado como Elo Tipo “T” com Área de Interesse definida na TCA 200-1;
- c) GABAER; e
- d) OM cujo Comandante seja designado como Comandante de Guarnição de Aeronáutica.

2.1.2 Poderão ser cadastrados no máximo 02 (dois) militares por OM.

2.1.3 As OM que não tiverem acesso ao INFOSEG, em caso de necessidade de consulta, deverão solicitar ao Escalão Superior que tenha acesso ao Sistema.

2.1.4 Os Comandantes das OM deverão informar ao CIAER, de imediato, sobre os militares que, por alguma razão, devam ser excluídos do acesso ao INFOSEG. Ex: transferências, substituições, outros.

2.2 REQUISITOS OBRIGATÓRIOS DOS INDICADOS

2.2.1 São requisitos obrigatórios para a indicação de acesso ao Sistema INFOSEG:

- a) Estar com a Credencial de Segurança válida;
- b) Pertencer à OM constituinte do Sistema de Inteligência da Aeronáutica (SINTAER) conforme estabelecido no item 2.1, com seu cadastro atualizado no Portal da Rede Mercúrio; e
- c) Ser Oficial, Suboficial ou Sargento de carreira, da Ativa ou Prestando Tarefa por Tempo Certo (PTTC).

2.3 PROCEDIMENTOS PARA O CADASTRAMENTO

Procedimentos	Responsável
Definir o(s) usuário(s) da OM para acesso ao Sistema INFOSEG.	Comandante de OM.
Formalizar via Ofício ao CIAER, informando nome, CPF, número SARAM e um telefone para contato, com o devido Termo de Compromisso de Manutenção do Sigilo, conforme ANEXO B, devidamente preenchido e assinado.	Comandante de OM.
Realizar o pré-cadastro no Sistema INFOSEG (https://seguranca.sinesp.gov.br/sinesp-seguranca/login.jsf)	Militar indicado pelo Cmt da OM.
Aprovar os militares indicados pelos Comandantes de OM.	Chefe do CIAER.

3 PROCEDIMENTOS PARA UTILIZAÇÃO

3.1 A utilização dos dados oriundos do INFOSEG somente poderá ocorrer para suprir as necessidades do serviço.

3.2 As consultas deverão estar vinculadas à necessidade de conhecer, objetivando obter informações fidedignas que contribuam para o processo de assessoria do Comandante. Tais consultas posteriormente serão informadas em um relatório mensal ao CIAER, assinado pelo comandante da OM ou seu substituto eventual, conforme Anexo A, por meio da Rede Mercúrio, até o segundo dia útil de cada mês, para eventuais auditorias. A não observância deste item poderá ocasionar o descredenciamento sumário do militar credenciado.

3.3 O setor de Inteligência da OM deverá comunicar ao CIAER a ocorrência de militares cadastrados no INFOSEG que deixaram de cumprir os requisitos em 2.2.1, gerenciando as supostas substituições, com a anuência do seu respectivo Comandante.

3.4 O setor de Inteligência da OM deverá comunicar ao CIAER a ocorrência de militares cadastrados no INFOSEG que passaram a responder a processo administrativo ou criminal.

4 NORMAS DE SEGURANÇA

4.1 POLÍTICA DE SENHAS

4.1.1 A senha não pode conter endereço de e-mail ou alguma parte do nome do usuário.

4.1.2 A senha deve ser alterada de 45 em 45 dias ou quando o próprio sistema exigir um prazo menor.

4.1.3 A senha nova nunca deve ser a mesma que as 04 últimas.

4.1.4 A senha não deve ser uma palavra comum.

4.1.5 A senha deverá ser criada pelo usuário e não deverá ser gerada por mecanismo automático.

4.1.6 As senhas devem conter, no mínimo, oito caracteres, utilizando números, caracteres especiais e letras maiúsculas e minúsculas.

4.1.7 Após a criação da senha de acesso, o militar deverá memorizá-la e não deverá copiá-la em nenhum meio físico ou lógico para que esta não possa ser utilizada por outra pessoa.

4.1.8 A sua senha pessoal não deverá ser divulgada sob qualquer hipótese à outra pessoa.

5 RESPONSABILIDADES DOS MILITARES CADASTRADOS

5.1 Durante o cadastramento “on-line”, o militar deverá atentar para a correta nomenclatura do e-mail pessoal, pois este será o único modo de comunicação da senha para o primeiro acesso ao Sistema.

5.2 O militar é o único responsável pelo uso indevido de sua senha, bem como pela utilização incorreta das informações contidas no Sistema.

5.3 O militar deverá assinar um termo de responsabilidade pelos seus atos e encaminhar junto ao ofício de solicitação ao INFOSEG.

5.4 O telefone autenticador deverá ser preferencialmente uma linha celular de serviço. Não utilizar os números de telefones fixos das OM que sejam habilitados por meio de central PABX, pois estes números inviabilizam a confirmação por parte do Sistema INFOSEG.

6 DISPOSIÇÕES FINAIS

6.1 A página inicial do INFOSEG traz uma série de informações importantes aos usuários. Porém, é importante atentar para a Lei Geral de Proteção de Dados (LGPD) que pactua diversos princípios e estabelece mecanismos para garantir a segurança de dados dos usuários, especialmente em relação ao direito à privacidade e ao controle de suas informações. Além disso, disciplina um conjunto de aspectos: define categorias de dados, circunscreve para quem valem seus ditames, fixa as hipóteses de coleta e tratamento de dados, traz os direitos dos titulares de dados e lista um conjunto de sanções para o caso de violação das regras previstas.

6.2 A critério do Ministério da Justiça e Segurança Pública, visando aprimorar o Sistema e sua segurança, a qualquer momento poderão ser tomadas novas medidas em relação ao acesso à Rede INFOSEG.

6.3 A critério do Ministério da Justiça e Segurança Pública ou por solicitação de autoridade competente, qualquer acesso ao Sistema INFOSEG pode ser alvo de auditoria, a fim de verificação de uso inadequado do sistema.

6.6 O Chefe do CIAER será o responsável pela avaliação final da necessidade do Elo de Inteligência de obter o acesso ao Sistema INFOSEG.

6.7 Os casos não previstos serão submetidos à deliberação do Chefe do CIAER.

REFERÊNCIAS

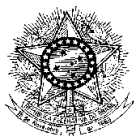
BRASIL. Presidência da República. Secretaria - Geral: Lei Geral de Proteção de Dados (LGPD). LEI N° 13.709. Brasília, 2018.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. PCA 16-14 – Plano de Adequação do Comando da Aeronáutica à Lei Geral de Proteção de Dados Pessoais. Brasília. 2021.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. TCA 200-1 – Organizações Militares do Sistema de Inteligência da Aeronáutica. Brasília. 2021.

DOCUMENTO PREPARATÓRIO – ACESSO RESTRITO

Art. 3º, Inciso XII e Art. 20 do Decreto nº 7.724, de 16 de maio de 2012

ANEXO A**MINISTÉRIO DA DEFESA****NOME DA ORGANIZAÇÃO MILITAR****RELATÓRIO MENSAL DE CONSULTAS NO SISTEMA INFOSEG****MÊS/ANO**

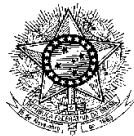
Data do Acesso	Qtde de Acessos	Tipo de Acesso (CPF, CNPJ, Placa...)	Solicitante	Motivo do Acesso
01/01/22	30	CPF	Cmt OM	Verificar a idoneidade de militar
02/01/22	01	Placa automotiva	Encarregado de IPM	Identificar proprietário de veículo que empreendeu fuga, após envolvimento em colisão com viatura orgânica.
TOTAL DE ACESSOS NO MÊS				31

Comandante da OM**DOCUMENTO PREPARATÓRIO – ACESSO RESTRITO**

Art. 3º, Inciso XII e Art. 20 do Decreto nº 7.724, de 16 de maio de 2012

DOCUMENTO PREPARATÓRIO – ACESSO RESTRITO

Art. 3º, Inciso XII e Art. 20 do Decreto nº 7.724, de 16 de maio de 2012

ANEXO B**MINISTÉRIO DA DEFESA
NOME DA ORGANIZAÇÃO MILITAR****TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO – INFOSEG**

(NOME COMPLETO)

(NACIONALIDADE)

(CPF)

(Nº IDENTIDADE)

(LOCAL DE EXPEDIÇÃO)

Perante o Comando da Aeronáutica, declaro ter ciência inequívoca do Sistema INFOSEG, cujo uso indevido possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário inerente ao seu acesso, além de:

- a) tratar as informações observadas no Sistema em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo Comando da Aeronáutica e preservar o seu sigilo, de acordo com a legislação vigente;
- b) preservar o conteúdo das informações observadas no sistema em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-los a terceiros;
- c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações observadas no Sistema em qualquer grau de sigilo, ou dos materiais de acesso restrito; e
- d) não copiar ou reproduzir, por qualquer meio ou modo: (i) informações observadas no Sistema em qualquer grau de sigilo; (ii) informações relativas aos materiais de acesso restrito do Comando da Aeronáutica, salvo com autorização da autoridade competente.

Declaro ainda que tenho conhecimento das normas e procedimentos discriminados na FCA 200-7.

Local , de de 2022.

Assinatura do declarante

DOCUMENTO PREPARATÓRIO – ACESSO RESTRITO

Art. 3º, Inciso XII e Art. 20 do Decreto nº 7.724, de 16 de maio de 2012