PORTARIA CGU Nº 1.129, DE 15.03.2019

Atualiza a Política de Credenciamento e Uso do Sistema de Investigação de Movimentação Bancária e do Sistema ARGUS no âmbito da Controladoria-Geral da União.

O SECRETÁRIO-EXECUTIVO DA CONTROLADORIA-GERAL DA UNIÃO, no exercício das atribuições instituídas nos incisos IV e VI do art. 5º do Anexo I ao Decreto nº 9.681, de 03 de janeiro de 2019, e considerando a necessidade de atualizar os procedimentos para a utilização do Sistema de Investigação de Movimentação Bancária - SIMBA e do Sistema ARGUS no âmbito da Controladoria-Geral da União - CGU, resolve:

Da Finalidade;

Art. 1º O acesso ao Sistema de Investigação de Movimentação Bancária - SIMBA e ao Sistema ARGUS no âmbito da CGU obedecerá às regras de credenciamento e uso dispostas nesta Portaria.

Art. 2º Para os fins desta Portaria, ficam estabelecidas as seguintes definições:

I - Sistema de Investigação de Movimentação Bancária - SIMBA: sistema informatizado, em ambiente de rede, que processa as solicitações, o recebimento e o trâmite de informações oriundas de pedidos de afastamento de sigilo bancário;

II - Sistema ARGUS: ferramenta informatizada de inteligência financeira e análise gráfica dos dados bancários recebidos pelo SIMBA;

III - Caso: a solicitação de afastamento de sigilo bancário, formulado por meio do sistema ARGUS e decorrente de investigação em curso na CGU, e as informações bancárias obtidas em razão deste afastamento, ao qual será atribuído um número pelo referido sistema;

IV - Quarentena: processo de validação das informações transmitidas pelas instituições financeiras;

V - Perfil Administrador: habilitação com privilégios de cadastro e gerenciamento de usuários;

VI - Perfil Chefia: habilitação com privilégios de criação e visualização de casos e de autorização para visualização destes;

VII - Perfil Auditor: habilitação com privilégios de visualização dos casos autorizados;

VIII - Perfil Quarentenista: habilitação com privilégios de acesso ao Gerente de Chaves de Acesso ao Sistema Transmissor - GCAST e quarentena dos dados transmitidos; e

IX - Gestor do sistema: área gestora responsável pela coordenação das ações relacionadas à utilização do SIMBA e do ARGUS no âmbito da CGU e pela interlocução junto aos demais órgãos partícipes.

Do Acesso;

Art. 3º Os perfis de acesso do SIMBA e do ARGUS serão concedidos da seguinte forma:

I - perfil Administrador: servidores efetivos designados pelo Diretor de Operações Especiais da Secretaria de Combate à Corrupção - SCC;

II - perfil Chefia:

a) Secretário Federal de Controle Interno Adjunto:

b) Secretário Federal de Combate à Corrupção Adjunto;

c) Diretor de Operações Especiais;

d) Diretor de Pesquisas e Informações Estratégicas;

e) Diretor de Acordos de Leniência;

f) Corregedor-Geral da União;

g) Diretor de Responsabilização de Entes Privados;

h) Diretor de Responsabilização de Agentes Públicos; e

i) Superintendentes das Controladorias Regionais da União nos Estados;

III - perfil Auditor: servidores efetivos que tenham necessidade de conhecer as informações sigilosas do caso, autorizados pelas autoridades que detêm perfil Chefia; e

IV - perfil Quarentenista: servidores efetivos designados pelas autoridades elencadas no inciso II.

1º O detentor do perfil Auditor será responsável imediato pela guarda e medidas de salvaguarda dos documentos resultantes de eventual extração de dados dos sistemas, podendo dar ciência de seu conteúdo a terceiros, uma vez justificada a necessidade de conhecer as informações sigilosas do caso, nas seguintes hipóteses:

a) no âmbito da Corregedoria-Geral da União - CRG, aos integrantes de comissões formalmente designadas para investigar o sujeito passivo a que se refere a informação bancária solicitada;

b) no âmbito da SCC, aos servidores que participem diretamente do trabalho de operações especiais, acordos de leniência ou informações estratégicas, incluídos aqueles que lotados nas Controladorias Regionais da União nos Estados; e

c) no âmbito da Secretaria Federal de Controle Interno - SFC, aos servidores que necessitem realizar ações de controle com vistas a verificar a efetividade dos programas do governo federal e da gestão dos recursos públicos federais sob a responsabilidade de órgãos e entidades públicos e privados.

2º Fica proibido o acesso aos sistemas SIMBA e ARGUS por empregados terceirizados, estagiários, prestadores de serviço, servidores inativos ou terceiros.

3º O pedido de acesso será formulado à chefia competente através do sistema SEI e deverá conter o login de rede, o endereço do correio eletrônico institucional do solicitante, o telefone de contato e o perfil de acesso desejado.

Art. 4º Compete à autoridade detentora do perfil Administrador:

I - cadastrar os usuários do sistema, nos termos do art. 3º; e

II - adotar as providências necessárias junto à Diretoria de Tecnologia da Informação - DTI para a manutenção e a atualização dos sistemas.

Art. 5º Compete às autoridades detentoras do perfil Chefia:

I - receber e processar as solicitações de criação, visualização ou alteração de casos;

II - autorizar, no âmbito de suas respectivas unidades, as solicitações de cadastramento de usuários

perfil Auditor; e

III - indicar, no âmbito de suas respectivas unidades, o servidor responsável pela quarentena das informações transmitidas pelas instituições financeiras.

Art. 6º Compete ao servidor com perfil Auditor:

I - solicitar ao usuário com perfil Chefia correspondente a autorização para criação de caso no sistema ARGUS; e

II - analisar as informações recebidas pelas instituições financeiras, quando concluído o processo de quarentena.

Parágrafo único. A solicitação de criação de caso nos sistemas SIMBA e ARGUS destinar-se-á exclusivamente:

a) no âmbito da CRG, à instrução de investigação patrimonial ou processo administrativo que requeira análise bancária;

b) no âmbito da SFC, à instrução de ações de controle que requeiram análises bancárias de contas públicas; e

c) no âmbito da SCC, à instrução de processo que verse sobre operação especial, investigação patrimonial ou acordo de leniência em andamento na CGU.

Art. 7º Compete ao Gestor do sistema:

I - supervisionar a utilização dos sistemas SIMBA e ARGUS no âmbito da CGU;

II - representar a CGU nos fóruns e eventos relacionados aos sistemas SIMBA e ARGUS;

III - representar a CGU perante os órgãos mantenedores dos sistemas SIMBA e ARGUS e os demais órgãos partícipes; e

IV - prestar apoio às unidades usuárias do sistema, no que lhe couber.

Art. 8º Compete ao servidor com perfil Quarentenista:

I - processar os pedidos de chaves formulados pelas instituições financeiras com vistas à transmissão dos dados bancários; e

II - realizar o processo de quarentena das informações enviadas pelas instituições financeiras relativas aos casos sob responsabilidade da sua unidade.

Art. 9º Compete a todos os servidores da CGU com perfil cadastrado nos sistemas SIMBA ou ARGUS:

I - utilizar as informações obtidas exclusivamente para os fins pelos quais foram solicitadas; e

II - zelar pelo sigilo das informações a que tenham acesso.

Da Criação do Caso;

Art. 10. O registro do pedido de afastamento de sigilo bancário deverá ser feito no sistema ARGUS, devendo constar, no mínimo:

I - a Secretaria de lotação do solicitante (campo Procuradoria);

II - nome do caso;

III - número do processo administrativo no Sistema Eletrônico de Informações - SEI;

IV - descrição dos fatos e justificativa pormenorizada; e

V - identificação dos investigados e eventuais terceiros que sejam de interesse para a investigação.

Art. 11. Caberá à autoridade detentora do perfil Chefia deliberar sobre o pedido de afastamento.

Art. 12. Caberá ao solicitante acompanhar o andamento do pedido judicial de afastamento ou compartilhamento de sigilo bancário junto ao Poder Judiciário e demais órgãos competentes.

Da Quarentena;

Art. 13. Compete ao servidor responsável pela Quarentena o recebimento e validação das informações bancárias transmitidas pelas instituições financeiras à CGU.

Art. 14. Para a validação das informações, o responsável pela Quarentena verificará a integridade, eventuais inconsistências, divergências e erros formais ou materiais que os dados recebidos possam conter.

Parágrafo único. Identificada incorreção ou insuficiência das informações, o responsável pela Quarentena comunicará o usuário Auditor responsável pelo caso e solicitará à instituição financeira correspondente os ajustes necessários.

Das Disposições Finais;

Art. 15. Compete à Diretoria de Operações Especiais da SCC a função de Gestor dos sistemas SIMBA e ARGUS no âmbito da CGU.

Art. 16. As informações constantes no SIMBA serão extraídas tão-somente para fins de instrução dos procedimentos administrativos correspondentes, vedada a sua reprodução ou gravação em pasta de rede pública, repositório em nuvem ou dispositivos particulares, sem a devida proteção criptográfica.

Art. 17. Todo aquele que tome conhecimento do conteúdo de documento sigiloso,

nos termos desta Portaria, fica responsável pela preservação do seu sigilo.

Parágrafo único. O acesso a documentos e processos sigilosos pelos servidores públicos efetivos elencados no rol do art. 3º desta Portaria acarreta a transferência da obrigação de preservar o sigilo, sob pena de responsabilização penal, civil e administrativa.

Art. 18. O acesso imotivado às informações dos sistemas SIMBA e ARGUS, assim entendido como aquele realizado para fins estranhos à investigação que deu origem ao caso, constitui infração funcional, sem prejuízo da responsabilidade civil e penal.

Art. 19. Ficam revogadas:

I - a Portaria CGU nº 263, de 2 de fevereiro de 2016; e

II - a Portaria CGU nº 2.174, de 10 de outubro de 2017.

Art. 20. Esta Portaria entra em vigor na data de sua publicação.

JOSE MARCELO CASTRO DE CARVALHO

(DOU de 19.03.2019 - pág. 31 - Seção 1)