NORMAS

Visão Original

PORTARIA COTEC Nº 54, DE 08 DE JUNHO DE 2017

(Publicado(a) no DOU de 22/06/2017, seção 1, página 21)

Dispõe sobre as formas e critérios de segurança da informação para o acesso a dados da Secretaria da Receita Federal do Brasil (RFB) por órgãos convenentes ou por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional.

A COORDENADORA-GERAL DE TECNOLOGIA DA INFORMAÇÃO, no uso da atribuição que lhe confere o inciso III do art. 312 do Regimento Interno da Secretaria da Receita Federal do Brasil, aprovado pela Portaria MF nº 203, de 14 de maio de 2012, e tendo em vista o disposto no art. 22, inciso VI, da Portaria SRF nº 450, de 28 de abril de 2004, o disposto na Portaria RFB nº 1.384, de 09 de setembro de 2016, na Portaria RFB nº 1.639, de 22 de novembro de 2016, e a necessidade de regulamentar as formas e critérios de segurança da informação para acesso a bases de dados da Secretaria da Receita Federal do Brasil por órgãos convenentes ou por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, resolve:

DISPOSIÇÕES PRELIMINARES

Art. 1º O modelo tecnológico para disponibilização de dados constantes de base de dados da Secretaria da Receita Federal do Brasil (RFB) para órgãos convenentes e órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional seguirá o disposto nesta Portaria.

Parágrafo Único. Para efeitos desta Portaria, além do disposto no artigo 2º da Portaria SRF nº 450/2004, entende-se por:

I - Forma de acesso: meio ou tecnologia utilizada para acessar as informações disponibilizadas a convenente ou a órgãos e entidades da administração pública federal direta, autárquica e fundacional;

II - Web Service/Application Programming Interface (API): Aplicação lógica, programável que torna compatíveis entre si diferentes aplicativos, independentemente do sistema operacional, arquitetura ou protocolo utilizados (REST ou SOAP), permitindo a comunicação e intercâmbio de dados entre diferentes redes e sistemas;

III - Perfil de sistema: conjunto de privilégios ou transações de um sistema atribuído a um usuário;

IV - Perfil de serviço: conjunto de privilégios e informações passíveis de consulta por meio de um serviço atribuído a um órgão convenente ou a órgãos e entidades da administração pública federal direta, autárquica e fundacional;

IV - Transação: conjunto de operações que desempenha uma função lógica em um sistema;

V - Evento: qualquer interação com o ambiente informatizado da RFB, com ou sem intervenção do usuário;

VI - Registro de eventos (log): conjunto de informações armazenadas para permitir o acompanhamento de eventos praticados no ambiente informatizado; e

VII - Apuração especial: procedimento computacional destinado a gerar relatório ou arquivo eletrônico especificado pela RFB e executado por um de seus prestadores de serviços.

DAS FORMAS DE ACESSO

Art. 2º O acesso aos dados da RFB, por órgãos convenentes ou por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, dar-se-á por consulta via Web Service/API, com o uso de certificado digital.

§ 1º Para dados do Cadastro de Pessoa Física (CPF) e do Cadastro Nacional de Pessoa Jurídica (CNPJ), em complemento ao disposto no caput, é facultado o acesso por meio de habilitação em perfis próprios desses sistemas, permitindo acesso aos seguintes dados:

I - CPF:

- Número de inscrição;

- Nome;

- Situação cadastral;

- Indicativo de residente no exterior;

- Nome do país, caso seja residente no exterior;

- Nome da mãe;

- Data de nascimento;

- Sexo;

- Endereço completo (tipo de logradouro, nome do logradouro, número da habitação, CEP, UF e município);

- Telefone;

- Unidade administrativa;

- Ano do óbito;

- Indicativo de estrangeiro;

- Data de inscrição do CPF;

- Naturalidade; e

- Nacionalidade.

II - CNPJ:

- Número de inscrição;

- Indicador de matriz/filial;

- Nome empresarial;

- Nome fantasia;

- Situação cadastral;

- Cidade no exterior, caso o estabelecimento seja domiciliado no exterior;

- Código do país, caso o estabelecimento seja domiciliado no exterior;

- Nome do país, caso o estabelecimento seja domiciliado no exterior;

- Data da situação cadastral;

- Natureza jurídica;

- Data de abertura;

- CNAE - Principal;

- CNAE secundários (até 10);

- Endereço:

- Telefone;

- E-mail;

- Responsável pela PJ, CPF e nome;

- Capital Social da Empresa;

- CPF dos participantes do QSA;

- Qualificação dos participantes no QSA; e

- Porte do estabelecimento.

§ 2º A disponibilização de acesso aos dados por meio de fornecimento de réplicas, parciais ou totais, das bases de dados do CPF e CNPJ, poderá ser realizada até 31 de dezembro de 2018, nos termos do § 2º do art. 6º da Portaria RFB nº 1639, de 2016.

§ 3º O órgão receptor das bases de dados de que trata o art. 2º deve garantir a total rastreabilidade das informações ou mídias fornecidas, em conformidade com os requisitos previstos nesta Portaria.

DOS CRITÉRIOS DE SEGURANÇA PARA ACESSO VIA WEB SERVICES

Art. 3º Os Web Services/API utilizados para o fornecimento dos dados deverão conter as seguintes funcionalidades e características:

I - comunicação via HTTPS com uso de certificado digital ICP-Brasil, emitido em nome do órgão receptor dos dados objeto de convênio ou autorização, do tipo e-Equipamento;

II - filtrar a conexão de origem por conjunto de endereços IP atribuídos aos órgãos receptores dos dados;

III - exigir a identificação (CPF) do usuário que está de fato realizando a consulta aos dados;

IV - habilitação em perfis de serviços e sistemas de acesso a base por órgãos convenentes ou por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, com vias a restringir o acesso apenas aos órgãos/usuários devidamente autorizados; e

V - registro de todos os eventos, com armazenamento e forma como definidas na Portaria RFB nº 693, de 13 de fevereiro de 2014.

DA HABILITAÇÃO EM PERFIS DE SISTEMAS

Art. 4º As habilitações de usuários de órgãos convenentes ou de órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, para acesso a sistemas da RFB seguirão o rito estabelecido na Portaria RFB/Sucor/Cotec nº 73, de 08 de dezembro de 2014, alterada pela Portaria RFB/Sucor/Cotec nº 1, de 11 de janeiro de 2016.

§ 1º As habilitações serão realizadas apenas por necessidade de serviço, as quais, após cessados os motivos que levaram a sua concessão, deverão ser retiradas por meio de uma solicitação de desabilitação.

§ 2º A qualquer tempo a RFB poderá solicitar aos órgãos convenentes ou por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional a revisão das habilitações vigentes dos seus usuários.

DA UTILIZAÇÃO E PROTEÇÃO DAS INFORMAÇÕES DISPONIBILIZADAS

Art. 5º O convenente e órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional são responsáveis pela correta utilização dos dados disponibilizados e os mesmos não poderão ser transferidos a terceiros, total ou parcialmente, ou divulgados de qualquer forma ou a qualquer título.

Art. 6º Os dados poderão ser utilizados apenas nas atividades intrínsecas para as quais foram solicitadas.

Art. 7º A utilização dos dados disponibilizados pela RFB em desconformidade com a legislação pertinente, implicará o imediato cancelamento da disponibilização, sem prejuízo de apurações de responsabilidade na forma prevista em regulamentação específica.

Art. 8º Os sistemas de informação de âmbito interno dos órgãos convenentes ou dos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, que consumirem as informações disponibilizadas, deverão implementar, no mínimo, os seguintes requisitos:

I - Acesso por meio de certificado digital ICP-Brasil, padrão A3;

II - Uso de protocolos criptografados para tráfego e armazenamento de dados;

III - Registro de todos os eventos de logs que envolvam os dados objetos do convênio ou autorização, permitindo identificar individualmente a operação efetuada, o usuário, estação de trabalho e data/hora das transações realizadas;

IV - Adoção dos meios necessários para promover criptografia dos backups operacionais;

V - Estabelecimento de perfis de acesso com definição de atribuições e responsabilidades dos usuários neles habilitados; e

VI - Acesso regulamentado mediante processos formais para a solicitação de acesso aos perfis dos sistemas, permitindo verificar, inclusive, os autorizadores que concederam as permissões ao usuário.

§ 1º Os órgãos convenentes ou os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional deverão guardar por período necessário à garantia de responsabilidade dos usuários por eventual uso indevido das informações, observadas as políticas e normas internas, os dados relativos ao controle de acesso e ao acesso a registros de informação, bem como os documentos referentes à autorização de acesso e utilização dos dados disponibilizados pela RFB.

§ 2º Deve ser adotado anualmente procedimentos formais para a revisão das habilitações concedidas.

§ 3º Os sistemas de que trata o caput devem ser desenvolvidos com adesão à práticas e metodologias de desenvolvimento seguro com vias a mitigar vulnerabilidades e falhas no sistema.

Art. 9. As salas, nos órgãos receptores dos dados ou prestadores de serviço, destinadas aos equipamentos servidores, banco de dados e storages responsáveis pela recepção e guarda dos dados provenientes da RFB, deverão implementar, no mínimo, os seguintes requisitos:

I - utilização de mecanismo eletrônico de identificação e controle de acesso baseado em, no mínimo, dois fatores de autenticação;

II - todo acesso de pessoas e materiais deve ser autorizado e registrado por equipamento de monitoramento, 24 horas pelos 7 dias da semana, e mantidas em arquivos de log;

III - infraestrutura protegida com ativos de segurança (Firewall, IDS - Intrusion Detection System e IPS - Intrusion Prevention System) e gerenciados e monitorados por Grupo de Resposta a Ataques - GRA; e

IV - manutenção das imagens do sistema de monitoramento, preferencialmente na mesma mídia, pelo período mínimo de um ano.

DAS DISPOSIÇÕES FINAIS

Art. 10. O convenente ou os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional devem garantir a implementação das políticas de segurança da informação dispostas nesta Portaria, sendo facultado à RFB solicitar, a qualquer momento, a demonstração do atendimento do disposto nesta Portaria.

Art. 11. Fica revogada a Portaria RFB/Sucor/Cotec nº 83, de 14 de dezembro de 2016.

Art. 12. Esta Portaria entra em vigor na data de sua publicação no Diário Oficial da União.

CLAUDIA MARIA DE ANDRADE