INFORMEF

JANEIRO/2022 - 2º DECÊNDIO - Nº 1928 - ANO 66

BOLETIM IMPOSTO DE RENDA/CONTABILIDADE

ÍNDICE

DECISÕES ADMINISTRATIVAS DA RECEITA FEDERAL DO BRASIL

INFORMEF DISTRIBUIDORA LTDA
Av. Dom Pedro II, 2.295 - Carlos Prates
CEP: 30.710-535 - BH - MG
TEl.: (31) 2121-8700
www.informef.com.br
Instagram: @informefdistribuidora

#IR6691#

VOLTAR

IR - FONTE - ARRENDAMENTO MERCANTIL DE AERONAVE OU DE MOTORES DESTINADOS A AERONAVES - REMESSA PARA O EXTERIOR - ALÍQUOTAS - REDUÇÃO - ALTERAÇÕES

MEDIDA PROVISÓRIA Nº 1.094, DE 31 DE DEZEMBRO DE 2021.

OBSERVAÇÕES INFORMEF

O Presidente da República, por meio da Medida Provisória nº 1.094/2021, altera a Lei nº 11.371/2006, que prevê, além de outros assuntos, sobre o imposto de renda na fonte incidente sobre os valores correspondentes aos pagamentos de contraprestação de arrendamento mercantil de bens de capital, celebrados com entidades mercantil de bens de capital, celebrados com entidades domiciliadas no exterior.

Essa alteração dispôs sobre a redução nas alíquotas deste imposto quando do pagamento, crédito, entrega, emprego ou remessa, por fonte situada no País, a pessoa jurídica domiciliada no exterior, a título de contraprestação de contrato de arrendamento mercantil de aeronave ou de motores destinados a aeronaves, celebrado por empresa de transporte aéreo público regular, de passageiros ou cargas.

Revoga o art. 21 da Lei nº 11.945/2009, art. 45 da Lei nº 12.431/2011 *(V. Bol. 1.550 - LEST), art. 89 da Lei nº 13.043/2014 *(V. Bol. 1.671 - LEST) e art. 1º da Lei nº 14.002/2020 *(V. Bol. 1.870 - LEST).

Altera a Lei nº 11.371, de 28 de novembro de 2006, para dispor sobre a redução na alíquota do imposto sobre a renda incidente sobre as operações que menciona.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º A Lei nº 11.371, de 28 de novembro de 2006, passa a vigorar com as seguintes alterações:

"Art. 16. Fica reduzida a alíquota do imposto sobre a renda na fonte incidente nas operações de que trata o inciso V do *caput* do art. 1º da Lei nº 9.481, de 13 de agosto de 1997, na hipótese de pagamento, crédito, entrega, emprego ou remessa, por fonte situada no País, a pessoa jurídica domiciliada no exterior, a título de contraprestação de contrato de arrendamento mercantil de aeronave ou de motores destinados a aeronaves, celebrado por empresa de transporte aéreo público regular, de passageiros ou cargas, para:

I - zero, de 1º de janeiro de 2022 a 31 de dezembro de 2023;

II - um por cento, de 1º de janeiro a 31 de dezembro de 2024;

III - dois por cento, de 1º de janeiro a 31 de dezembro de 2025; e

IV - três por cento, de 1º de janeiro a 31 de dezembro de 2026." (NR)

Art. 2º Ficam revogados:

I - o art. 21 da Lei nº 11.945, de 4 de junho de 2009;

II - o art. 45 da Lei nº 12.431, de 24 de junho de 2011;

III - o art. 89 da Lei nº 13.043, de 13 de novembro de 2014; e

IV - o art. 1º da Lei nº 14.002, de 22 de maio de 2020.

Art. 3º Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 31 de dezembro de 2021; 200º da Independência e 133ºda República.

JAIR MESSIAS BOLSONARO
Marcelo Pacheco dos Guaranys
Marcelo Sampaio Cunha Filho

(DOU EDIÇÃO EXTRA G, 31.12.2021)

#IR6690#

VOLTAR

ESTATUTO NACIONAL MICROEMPRESA E EMPRESA DE PEQUENO PORTE - MODIFICAÇÃO DA COMPOSIÇÃO E FUNCIONAMENTO - COMITÊ GESTOR DO SIMPLES NACIONAL CGSN - AMPLIAÇÃO DO ÂMBITO DO SEU REGIME TRIBUTÁRIO - MEI CAMINHONEIRO - ALTERAÇÃO

LEI COMPLEMENTAR Nº 188, DE 31 DE DEZEMBRO DE 2021.

OBSERVAÇÕES INFORMEF

O Presidente da República, por meio da Lei Complementar nº 188/2021, altera a Lei Complementar nº 123/2006, estabelecendo que, para o transportador autônomo de cargas inscrito como MEI, o limite da receita bruta será de R$ 251.600,00 (duzentos e cinquenta e um mil e seiscentos reais); o limite será de R$ 20.966,67 (vinte mil novecentos e sessenta e seis reais e sessenta e sete centavos), multiplicados pelo número de meses entre o início da atividade e o final do respectivo ano-calendário, consideradas as frações de meses como um mês inteiro, sendo o valor da contribuição previdenciária correspondente a 12% (doze por cento) sobre o salário-mínimo mensal.

Altera a Lei Complementar nº 123, de 14 de dezembro de 2006 (Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte), para modificar a composição e o funcionamento do Comitê Gestor do Simples Nacional (CGSN) e ampliar o âmbito de aplicação de seu regime tributário.

O PRESIDENT E DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei Complementar:

Art. 1º A Lei Complementar nº 123, de 14 de dezembro de 2006, passa a vigorar com as seguintes alterações:

"Art. 2º .....

I - Comitê Gestor do Simples Nacional, vinculado ao Ministério da Economia, composto de 4 (quatro) representantes da União, 2 (dois) dos Estados e do Distrito Federal, 2 (dois) dos Municípios, 1 (um) do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae) e 1 (um) das confederações nacionais de representação do segmento de microempresas e empresas de pequeno porte referidas no art. 11 da Lei Complementar nº 147, de 7 de agosto de 2014, para tratar dos aspectos tributários;

.....

§ 4º Os comitês de que tratam os incisos I e III do *caput* deste artigo elaborarão seus regimentos internos mediante resolução, observado, quanto ao CGSN, o disposto nos §§ 4º-A e 4º-B deste artigo.

§ 4º-A. O quórum mínimo para a realização das reuniões do CGSN será de 3/4 (três quartos) dos componentes, dos quais um deles será necessariamente o Presidente.

§ 4º-B. As deliberações do CGSN serão tomadas por 3/4 (três quartos) dos componentes presentes às reuniões, presenciais ou virtuais, ressalvadas as decisões que determinem a exclusão de ocupações autorizadas a atuar na qualidade de Microempreendedor Individual (MEI), quando a deliberação deverá ser unânime.

.....

§ 8º Os membros dos comitês de que tratam os incisos I e III do *caput* deste artigo serão designados pelo Ministro de Estado da Economia, mediante indicação dos órgãos e entidades vinculados.

§ 8º-A. Dos membros da União que compõem o comitê de que trata o inciso I do *caput* deste artigo, 3 (três) serão representantes da Secretaria Especial da Receita Federal do Brasil e 1 (um) da Subsecretaria de Desenvolvimento das Micro e Pequenas Empresas, Empreendedorismo e Artesanato da Secretaria Especial de Produtividade e Competitividade ou do órgão que vier a substituí-la.

§ 8º-B. A vaga das confederações nacionais de representação do segmento de microempresas e empresas de pequeno porte no comitê de que trata o inciso I do *caput* deste artigo será ocupada em regime de rodízio anual entre as confederações.

....." (NR)

"Art. 18-A. .....

§ 1º Para os efeitos desta Lei Complementar, considera-se MEI quem tenha auferido receita bruta, no ano-calendário anterior, de até R$ 81.000,00 (oitenta e um mil reais), que seja optante pelo Simples Nacional e que não esteja impedido de optar pela sistemática prevista neste artigo, e seja empresário individual que se enquadre na definição do art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), ou o empreendedor que exerça:

I - as atividades de que trata o § 4º-A deste artigo;

II - as atividades de que trata o § 4º-B deste artigo estabelecidas pelo CGSN; e
III - as atividades de industrialização, comercialização e prestação de serviços no âmbito rural.
....." (NR)

Art. 2º A Lei Complementar nº 123, de 14 de dezembro de 2006 (Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte), passa a vigorar acrescida do seguinte art. 18-F:

"Art. 18-F. Para o transportador autônomo de cargas inscrito como MEI, nos termos do art. 18-A desta Lei Complementar:
I - o limite da receita bruta de que trata o § 1º e o inciso V do § 3º do art. 18-A desta Lei Complementar será de R$ 251.600,00 (duzentos e cinquenta e um mil e seiscentos reais);
II - o limite será de R$ 20.966,67 (vinte mil novecentos e sessenta e seis reais e sessenta e sete centavos) multiplicados pelo número de meses compreendidos entre o início da atividade e o final do respectivo ano-calendário, consideradas as frações de meses como um mês inteiro, no caso de início de atividades de que trata o § 2º do art. 18-A desta Lei Complementar;
III - o valor mensal da contribuição de que trata o inciso X do § 1º do art. 13 desta Lei Complementar corresponderá ao valor resultante da aplicação da alíquota de 12% (doze por cento) sobre o salário-mínimo mensal."

Art. 3º Esta Lei Complementar entra em vigor na data de sua publicação.
Brasília, 31 de dezembro de 2021; 200º da Independência e 133º da República.

JAIR MESSIAS BOLSONARO
Marcelo Pacheco dos Guaranys

(DOU EDIÇÃO EXTRA G, 31.12.2021)

BOIR6690---WIN/INTER

#IR6692#

VOLTAR

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS (CRCMG) - DADOS PESSOAIS NO ÂMBITO DO CRCMG - TRATAMENTO INTERNO - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

RESOLUÇÃO CRCMG Nº 435, DE 17 DE DEZEMBRO DE 2021.

OBSERVAÇÕES INFORMEF

O Conselho Regional de contabilidade de Minas Gerais, por meio da Resolução CRCMG n° 435/2021, instituiu a Política Interna de Proteção de Dados Pessoais do CRCMG, cujo objetivo é orientar todos aqueles que atuam tanto na qualidade de controlador quanto como operadores acerca das boas práticas em proteção de dados pessoais. A referida Resolução tem por finalidade estabelecer diretrizes para o tratamento interno de dados pessoais no âmbito do CRCMG, em conformidade com a Lei n.º 13.70/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

Institui a Política Interna de Proteção de Dados Pessoais do CRCMG.

O CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS, no exercício de suas atribuições legais e regimentais,
Considerando a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);
Considerando a necessidade de estabelecer diretrizes para o tratamento interno de dados pessoais no âmbito do CRCMG, a fim de atender aos dispositivos e estar em conformidade com a Lei Geral de Proteção de Dados Pessoais;
RESOLVE:

CAPÍTULO I
POLÍTICA E DEFINIÇÕES

Art. 1º Fica instituída a Política Interna de Proteção de Dados Pessoais do Conselho Regional de Contabilidade de Minas Gerais (CRCMG).
Art. 2º Para os efeitos desta resolução, entende-se por:

I - Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso significa que um dado é considerado pessoal quando permite a identificação direta ou indireta da pessoa natural;

II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

IV - Tratamento: toda a operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transparência, difusão ou extração;

V - Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No caso desta política, o CRCMG;

VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - Relatório de impacto à proteção de dados pessoais: documento de comunicação e transparência que orienta a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

CAPÍTULO II
OBJETIVO E PRINCÍPIOS

Art. 3º A Política Interna de Proteção de Dados Pessoais do CRCMG tem por objetivo orientar todos aqueles que atuam tanto na qualidade de controlador quanto como operadores acerca das boas práticas em proteção de dados pessoais, a fim propiciar conformidade com a Lei n.º 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 4º São princípios norteadores da LGPD e desta Política Interna:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO III
RESPONSABILIDADE E TRATAMENTO DE DADOS PESSOAIS

Art. 5º São responsáveis pelo correto tratamento dos dados pessoais o CRCMG, na qualidade de controlador, e todos aqueles que atuam como operadores, sendo necessária a cooperação dos envolvidos para o atendimento aos dispositivos legais e segurança dos dados pessoais sob seu controle.

Art. 6º O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, conforme disposto no artigo 42 e seguintes da LGPD.

Art. 7º O tratamento dos dados pessoais no CRCMG deve seguir os princípios definidos nesta política, devendo ser estritamente voltado às finalidades às quais a coleta dos dados se destina, respeitando os critérios de compartilhamento e de segurança das informações.

Art. 8º Os dados pessoais devem ser manipulados apenas por pessoas que precisem lidar com eles, reduzindo, assim, os riscos de falhas humanas propiciarem um vazamento ou uso inadequado da informação.

Art. 9º Os dados serão identificados por setores e/ou por responsabilidades específicas dentro de cada unidade operacional, a fim de se conhecer, em cada situação, aqueles que atuam na qualidade de controlador ou como operadores, reduzindo os riscos de um incidente na segurança da informação.

Art. 10. O acesso dos empregados e prestadores de serviço do CRCMG aos materiais e às informações contidas nos sistemas informatizados é restrito de acordo com a autorização determinada para cada colaborador, conforme definido na Política de Controle de Acesso Lógico do CRCMG.

Art. 11. O acesso de empregados ou prestadores de serviço ao banco de dados do CRCMG é individual e protegido por senha própria e intransferível, garantindo o tratamento dos dados a pessoas autorizadas, conforme as permissões de acesso pré-definidas.

Art. 12. O único tratamento admitido para dados pessoais contidos nos resíduos eletrônicos gerenciados pelo CRCMG é a eliminação.

Parágrafo único. Para garantir que nenhum dos dados que eventualmente estejam armazenados nos dispositivos que o CRCMG gerencia sejam utilizados indevidamente, todos serão destruídos em conformidade com a legislação arquivística vigente que trata sobre a matéria.

CAPÍTULO IV
CRITÉRIOS ESTABELECIDOS

Seção I
Para a coleta dos dados pessoais

Art. 13. As informações referentes às pessoas físicas somente devem ser coletadas na medida da necessidade para a prestação de serviços, em conformidade com as hipóteses constantes no artigo 7º da LGPD.

Art. 14. O consentimento, quando necessário, é requerido ao solicitar dados que forem de pessoas físicas, por meio do aceite no campo apropriado em sistema ou por meio de assinatura de termo apropriado.

Seção II
Para o armazenamento dos dados pessoais

Art. 15. Os dados pessoais serão armazenados seguindo as diretrizes da Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do CRCMG e a legislação arquivística vigente.

Art. 16. Quando armazenados fisicamente, os dados devem ficar em local protegido por tranca, fora do alcance de outras pessoas que não as expressamente autorizadas a acessá-los. Quando armazenados digitalmente, devem ficar em pasta protegida por criptografia ou restrição de acesso por senha pessoal, quando não se tratar de informações públicas.

Art. 17. Eventuais cópias de dados pessoais somente devem ser feitas, em caso de necessidade, para cumprimento da finalidade proposta ao tratamento dos dados.

Seção III
Para o compartilhamento interno e externo de dados pessoais

Art. 18. Os dados pessoais somente podem ser compartilhados internamente entre as Unidades Organizacionais cuja função exija acesso e tenha a finalidade ou a obrigação legal para o tratamento dessas informações.

Art. 19. O compartilhamento de dados pessoais com pessoa natural ou jurídica, de direito público ou privado, externas ao CRCMG deve ser restrito ao mínimo necessário para a execução do tratamento a que se destina, em cumprimento às hipóteses previstas na LGPD.

Parágrafo único. Mesmo quando o tratamento envolver diretamente a prestação de serviços, o consentimento para este tratamento e compartilhamento deverá ter sido previamente obtido, quando cabível e sempre que possível.

Art. 20. É vedado o compartilhamento externo de dados pessoais por qualquer meio, telefônico, digital ou por escrito, não amparado em base legal.

Seção IV
Para a eliminação dos dados pessoais

Art. 21. Quando atingida sua finalidade, os dados pessoais que não precisam ser armazenados para atendimento a exigências legais deverão ser eliminados, física e digitalmente, com a comunicação dessa eliminação ao titular, nos casos não previstos na legislação arquivística vigente ou quando ocorrerem de maneira diversa ao previsto no termo de consentimento aplicável.

CAPÍTULO V
ENCARREGADO E PRESTAÇÃO DE INFORMAÇÕES

Art. 22. O encarregado da Proteção de Dados Pessoais será o responsável pela comunicação entre os titulares, o CRCMG e a ANPD, conforme disposto na legislação vigente.

Art. 23. As atividades do encarregado consistem, conforme o artigo 41 da LGPD, em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Art. 24. A solicitação quanto à prestação de informações sobre dados pessoais deverá ser encaminhada ao encarregado de proteção de dados pessoais do CRCMG, para que este responda ao titular dos dados.

Art. 25. As informações requeridas pelo titular deverão ser sempre evidenciadas de forma transparente, resguardando o sigilo, quando aplicável.

Art. 26. Quaisquer questionamentos surgidos acerca da proteção de dados pessoais deverão ser levados ao encarregado para que este possa orientar de imediato o operador ou buscar junto à ANPD e demais entidades especializadas uma orientação adequada ao questionamento levantado.

Art. 27. O encarregado manterá relatório de avaliação de riscos e impactos à proteção de dados pessoais, por meio do qual as medidas necessárias à segurança da informação de dados pessoais poderão ser estruturadas, implementadas e avaliadas.

Art. 28. O encarregado de proteção de dados pessoais do CRCMG estará disponível por meio do sistema eletrônico constante na página www.crcmg.org.br/lgpd.

Art. 29. Esta resolução entra em vigor na data da sua publicação. Aprovada na 12º Reunião Plenária, realizada em 17 de dezembro de 2021.

ROSA MARIA ABREU BARROS
Presidente do Conselho

(DOU, 05.01.2022)

BOIR6692---WIN/INTER

#IR6693#

VOLTAR

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS (CRCMG) - POLÍTICA DE ARMAZENAMENTO DE DADOS - DOCUMENTOS E ARQUIVOS (PADDA) DO CRCMG - APROVAÇÃO

RESOLUÇÃO CRCMG Nº 437, DE 17 DE DEZEMBRO DE 2021.

OBSERVAÇÕES INFORMEF

O Conselho Regional de Contabilidade de Minas Gerais, por meio da Resolução CRCMG nº 437/2021, instituiu a Política de Armazenamento de Dados, Documentos e Arquivos (PADDA), cujo o objetivo é estabelecer as melhores práticas para o manuseio e o armazenamento de documentos não digitais e arquivos digitais do CRCMG.

Aprova a Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do CRCMG e dá outras providências.

O CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS, no uso de suas atribuições legais e regimentais,

Considerando a necessidade de estabelecer diretrizes e padrões para garantir um ambiente digital e não digital controlado, eficiente e seguro, de forma a oferecer todas as informações necessárias à classe contábil e à sociedade com integridade, confidencialidade e disponibilidade;

Considerando que o Conselho Regional de Contabilidade de Minas Gerais recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado;

Considerando que as informações no CRCMG são armazenadas em diferentes formas, veiculadas em diferentes meios físicos e eletrônicos, sendo, portanto, vulneráveis a incidentes, como casos fortuitos e de força maior, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

Considerando o número progressivo de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança a informação;

Considerando a Lei Federal nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD), de 14 de agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural";

Considerando o Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação, em especial o inciso II do artigo 15;

Considerando o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

Considerando a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Considerando a Resolução Conarq nº 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (Sinar);

Considerando a Resolução Conarq nº 38, de 9 de julho de 2013, que dispõe sobre a adoção das "Diretrizes do Produtor - A Elaboração e a Manutenção de Materiais Digitais: Diretrizes Para Indivíduos" e "Diretrizes do Preservador - A Preservação de Documentos Arquivísticos digitais: Diretrizes para Organizações";

Considerando a Recomendação Técnica do Arquivo Nacional nº 2, de junho de 2019, que dispõe sobre as Recomendações para Elaboração de Política de Preservação Digital;

Considerando a necessidade de estabelecer responsabilidade interna quanto ao armazenamento de dados, documentos e arquivos; resolve:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Seção I
PREMISSAS

Art. 1º Fica instituída a Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade de Minas Gerais (CRCMG), nos termos desta resolução.

Parágrafo único. Todos os instrumentos normativos gerados a partir da PADDA do CRCMG são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos.

Art. 2º A PADDA do Conselho Regional de Contabilidade de Minas Gerais se aplica a todos os conselheiros, empregados, estagiários, menores aprendizes, prestadores de serviços e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCMG e que tenham acesso a qualquer documento, arquivo e meio de informação e comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Art. 3º A PADDA tem por objeto garantir condições para que conselheiros, empregados, estagiários, menores aprendizes, colaboradores e, quando aplicável, terceiros e quaisquer outras pessoas que prestem serviços ao CRCMG sejam orientados sobre a existência e a utilização dos instrumentos normativos, procedimentos e controles de uso e armazenamento adotados pelo CRCMG.

Art. 4º As diretrizes desta política visam assegurar que dados, documentos e arquivos digitais e não digitais de uso sensível e/ou sigiloso sejam armazenados de modo a garantir a sua recuperação, integridade e

autenticidade, sendo removidos do espaço de trabalho do usuário e guardados quando não estiverem em uso ou em períodos de ausência do usuário, mesmo que momentânea.

Seção II
OBJETIVOS

Art. 5º Esta política tem o objetivo de estabelecer as melhores práticas para o manuseio e o armazenamento de documentos não digitais e arquivos digitais do CRCMG.

Parágrafo único. A PADDA está alinhada às estratégias instituticionais, à política de governança, à gestão de riscos e aos normativos que regem a matéria.

Art. 6º A PADDA trata do uso e do armazenamento de dados, arquivos e documentos no âmbito do CRCMG, em todo o seu ciclo de vida, objetivando à continuidade dos processos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação.

Art. 7º Para a segurança do uso e do armazenamento da informação no CRCMG, serão rigorosamente observados o compromisso institucional com a proteção das informações de sua propriedade e/ou sob sua guarda, a participação e o cumprimento por todos os colaboradores em todo o processo e o disposto neste normativo, nas disposições constitucionais, legais e regimentais vigentes.

Seção III
PRINCÍPIOS BÁSICOS

Art. 8º Com este PADDA, o CRCMG compromete-se com os seguintes princípios básicos:

I - desempenhar o papel de um custodiador de confiança dos documentos digitais e não digitais recolhidos e inseridos nos seus repositórios;

II - atuar com neutralidade, ou seja, demonstrar que não tem razões para alterar os documentos sob sua custódia e que não permitirá que outros alterem esses documentos, acidental ou propositalmente;

III - implantar um sistema de uso, armazenamento e preservação confiável, capaz de garantir a autenticidade dos documentos;

IV - garantir a preservação de todos os componentes digitais e não digitais dos documentos produzidos, recebidos e armazenados, de modo a permitir a apresentação desses documentos no futuro;

V - identificar explicitamente e garantir o grau de sigilo e a restrição de acesso à informação sensível relacionados aos documentos produzidos, recebidos e armazenados;

VI - gerenciar, no repositório, a permissão de acesso de documentos com grau de sigilo e/ou que registrem informação sensível, de acordo com legislação vigente e as normas de controle de acesso definidas no âmbito do CRCMG. Essas restrições devem ser registradas em metadados e procedimentos de acesso às áreas de armazenamento de dados, documentos e arquivos do CRCMG.

Seção IV
ABRANGÊNCIA

Art. 9º O disposto neste instrumento será aplicado a todos os conselheiros, empregados, estagiários, menores aprendizes, terceirizados e colaboradores que prestem serviços ao CRCMG e que tenham acesso a qualquer informação ou comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação.

CAPÍTULO II
DOS CONCEITOS E DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Seção I
CONCEITOS E DEFINIÇÕES

Art. 10. Para os efeitos desta Política de Armazenamento de Dados, Documentos e Arquivos, entende-se por:

I - Acessibilidade: facilidade no acesso ao conteúdo e ao significado de um objeto digital;

II - Armazenamento digital: guarda de documentos digitais em dispositivos de memória não volátil;

III - Armazenamento: guarda de documentos em local apropriado;

IV - Arquivamento: sequência de operações intelectuais e físicas que visam à guarda ordenada de documentos;

V - Arquivo digital: conjunto de bits que formam uma unidade lógica interpretável por um programa de computador e armazenada em suporte apropriado;

VI - Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

VII - Custódia: responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade;

VIII - Custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

IX - Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado;

X - Documento arquivístico: documento produzido ou recebido no curso de uma atividade prática como instrumento ou resultado dessa atividade, retido para ação ou referência;

XI - Documento digital: informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional;

XII - Documento não digital: documento que se apresenta em suporte, formato e codificação diferente dos digitais, tais como documentos em papel, documentos em películas e documentos eletrônicos analógicos;

XIII - Fidedignidade: credibilidade de um documento arquivístico como uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;

XIV - Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação;

XV - Incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

XVI - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

XVII - Integridade: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencionais ou acidentais, em seu estado e atividades;

XVIII - Metadados: dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

XIX - Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

XX - Preservação: prevenção da deterioração e danos em documentos, documentos por meio de adequado controle ambiental e/ou tratamento físico e/ou químico;

XXI - Preservação digital: conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário;

XXII - Recurso criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXIII - Repositório arquivístico digital: repositório digital que armazena e gerencia documentos arquivísticos, seja nas idades corrente e intermediária, seja na idade permanente;

XXIV - Repositório arquivístico digital confiável: é o repositório que deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável;

XXV - Repositório digital: complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, *software* e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos;

XXVI - Repositório digital confiável: é um repositório digital que é capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário;

XXVII - Risco: possibilidade potencial de uma ameça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

XXVIII - Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

XXIX - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXX - Unidade Gestora de Segurança da Informação: é a unidade responsável pela gestão de segurança da informação no CRCMG;

XXXI - Unidade Organizacional: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz;

XXXII - Usuários: pessoa física ou jurídica que opera algum sistema informatizado do Conselho Regional de Contabilidade de Minas Gerais;

XXXIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças.

Seção II
CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 11. A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrangem informações provenientes dos serviços essenciais de Tecnologia da Informação do CRCMG.

Parágrafo único. As informações devem ser classificadas de forma a permitir tratamento diferenciado de acordo com o seu grau de importância, criticidade, sensibilidade e em conformidade com os requisitos legais.

Art. 12. As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

I - Pública: são informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico, editais de licitação, agendas e rotinas;

II - Interna: são informações disponíveis aos colaboradores do CRCMG para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo, em especial, memorandos, portarias, procedimentos internos, avisos e campanhas internas;

III - Sigiloso: são informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros, em especial, processos judiciais e dados cadastrais de colaboradores;

IV - Sigiloso/restrito: são informações de acesso restrito a um colaborador ou grupo de colaboradores que, obrigatoriamente, são destinatários. Em geral, informações associadas ao interesse estratégico do CRCMG estão restritas ao presidente, à diretoria, aos gerentes e colaboradores cujas funções requeiram conhecê-las.

CAPÍTULO III
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
COMPETÊNCIAS

Art. 13. À Gerência de Tecnologia da Informação (Getin) compete:

I - promover e estruturar a preservação e o armazenamento dos documentos arquivísticos digitais, nas fases corrente, intermediária e permanente, que devem estar associadas a um repositório digital confiável para a gestão, a preservação e o acesso;

II - elaborar plano de ação para disponibilizar os repositórios digitais confiáveis para a gestão, a preservação e o acesso de documentos digitais, de acordo com as diretrizes previstas na Resolução n.º 39, de 29 de abril de 2014 do Conselho Nacional de Arquivos (Conarq);

III - implantar os parâmetros para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade, identidade, integridade, confidencialidade, disponibilidade, o acesso e a preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos de tempo ou, até mesmo, permanentemente.

Seção II
RESPONSABILIDADES

Subseção I
USUÁRIOS

Art. 14. Os usuários e quaisquer outras pessoas que prestem serviços ao CRCMG e tenham acesso ao ambiente de uso e armazenamento de dados, documentos e arquivos digitais e não digitais do Conselho têm as seguintes responsabilidades:

I - ter pleno conhecimento e cumprir fielmente esta política, as normas e os procedimentos de uso e armazenamento do CRCMG;

II - solicitar esclarecimentos ao Comitê Gestor de Privacidade e Proteção de Dados, em caso de dúvidas relacionadas a esta política;

III - gerenciar os dados, documentos e arquivos digitais e não digitais sob sua responsabilidade e garantir que os dados, documentos e arquivos não digitais ou digitais, equipamentos e recursos tecnológicos à sua disposição permaneçam seguros;

IV - armazenar documentos não digitais em ambientes seguros, não devendo permanecer sobre a mesa de trabalho do usuário quando não estiver em uso, ou em locais onde pessoas não autorizadas tenham acesso ao seu conteúdo;

V - remover do espaço de trabalho dados, informações, documentos e arquivos sensíveis e/ou sigilosas quando ausente, mesmo que momentaneamente, e ao final do dia de trabalho;

VI - manter trancados armários com documentos sensíveis e/ou sigilosos quando não estiverem em uso;

VII - manter em sigilo as chaves/senhas/credenciais usadas para acesso a informações, documentos e arquivos sensíveis;

VIII - evitar a impressão de documentos que contenham informações sensíveis e/ou sigilosas. Em caso de impressão, remover imediatamente da impressora;

IX - restituir prontamente os documentos recebidos por empréstimo de outras unidades, quando não forem mais necessários;

X - utilizar recursos de criptografia, sempre que possível, e guardar em locais seguros de armazenamento documentos que contenham informações sensíveis e/ou sigilosas;

XI - salvar e armazenar dentro de pasta ou unidade lógica específicas documentos que contenham dados pessoais;

XII - zelar pela custódia de dados e informações institucionais e evitar o salvamento de conteúdos e informações pessoais em máquinas e espaço físico do Conselho;

XIII - garantir que todas as informações não digitais e digitais sejam mantidas e armazenadas em local seguro quando não estiverem em uso;

XIV - armazenar os documentos que contenham dados pessoais somente pelo período necessário ao seu uso ou cumprimento do seu dever legal e prazos de guarda e locais indicados na Tabela de Temporalidade de Documentos utilizada no CRCMG;

XV - seguir os procedimentos e a legislação vigente para a eliminação de documentos digitais e não digitais do CRCMG;

XVI - estar ciente de que toda informação digital ou não digital armazenada, processada e transmitida no ambiente computacional ou físico do CRCMG pode ser auditada.

Subseção II
CUSTODIANTE

Art. 15. Ao custodiante da informação cabem as seguintes responsabilidades:

I - cumprir e zelar pela observância integral das diretrizes desta política e demais normas e procedimentos decorrentes;

II - zelar pela disponibilidade, integridade e confidencialidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta política e demais normas e procedimentos referentes ao uso e armazenamento de dados, documentos e arquivos;

III - participar de capacitação e treinamento em procedimentos de uso e armazenamento de dados, documentos e arquivos, quando convocado;

IV - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

V - comunicar prontamente ao seu gestor imediato e ao Comitê de Segurança da Informação qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, integridade e confidencialidade das informações armazenadas.

Subseção III
GESTORES DAS UNIDADES ORGANIZACIONAIS

Art. 16. Os Gestores das Unidades Organizacionais são responsáveis por:

I - ter postura exemplar em relação ao uso e armazenamento de dados, documentos e arquivos, para servir como modelo de conduta para os colaboradores sob sua gestão;

II - cumprir e fazer cumprir esta política;

III - adotar os procedimentos necessários sempre que identificar descumprimentos da política.

CAPÍTULO IV
DIVULGAÇÃO E ATUALIZAÇÃO

Art. 17. Esta política e suas atualizações, após publicação, deverão ser amplamente divugadas aos usuários e disponibilizadas no portal do CRCMG, sendo consideradas um documento de relevante interesse público.

Art. 18. Esta Política de Armazenamento de Dados, Documentos e Arquivos deverá ser revisada sempre que se fizer necessário.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 19. Os casos omissos desta política serão resolvidos pelo Comitê Gestor de Privacidade e Proteção de Dados do CRCMG.

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

Aprovada na 12ª Reunião Plenária, realizada em 14 de dezembro de 2021.

ROSA MARIA ABREU BARROS
Presidente do Conselho

(DOU, 05.01.2022)

BOIR6693---WIN/INTER

#IR6694#

VOLTAR

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS (CRCMG) - POLÍTICA DE INCIDENTES DE SEGURANÇA DA INFORMAÇÕES - DISPOSIÇÕES

RESOLUÇÃO CRCMG Nº 439, DE 17 DE DEZEMBRO DE 2021.

OBSERVAÇÕES INFORMEF

O Conselho Regional de Contabilidade de Minas Gerais, por meio da Resolução CRCMG n° 439/2021, instituiu a Política de Incidentes de Segurança da Informação do CRCMG, que visa estabelecer princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação digital e não digital do CRCMG.

A referida Resolução tem por objetivos:

a) diminuir os danos totais causados por incidentes que não puderam ser evitados, bem como a sua reincidência;

b) promover a efetiva e eficaz Política da Segurança da Informação no CRCMG; e

c) diminuir o número total de incidentes de segurança da informação envolvendo o CRCMG, por meio de prevenção sistemática dos eventos e eliminação de situações que permitam a ocorrência desses incidentes.

Institui a Política de Incidentes de Segurança da Informação do CRCMG.

O CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS, no exercício de suas atribuições legais e regimentais,

Considerando a Lei nº 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

Considerando que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta política em relação aos dados pessoais, mesmo após o seu término; resolve:

CAPÍTULO I
POLÍTICA E DEFINIÇÕES

Art. 1º Fica instituída a Política de Incidentes de Segurança da Informação do Conselho Regional de Contabilidade de Minas Gerais (CRCMG).

Art. 2º A Política de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação do CRCMG e visa orientar o funcionamento do processo de gestão de incidentes de segurança digital e não digital da informação, de forma que sejam tratados adequadamente, reduzindo ao máximo os impactos para a entidade.

Art. 3º Para os efeitos desta resolução, entende-se por:

I - Atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

II - Atividade crítica: atividade que deve ser executada de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permita atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - Atividade maliciosa: qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema, serviço ou rede;

IV - Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;

V - Colaborador: pessoa física ou jurídica envolvida em qualquer atividade do CRCMG, seja de natureza permanente, temporária ou excepcional, sendo delegado seccional, membro de Grupo de Estudos Técnicos, estagiário ou prestador de serviços;

VI - Evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas, ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;

VII - Fluxo de Trabalho de Incidentes: predefinição de etapas que devem ser tomadas para lidar com um tipo particular de incidente;

VIII - Gerenciamento de incidentes: processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidente garante que a operação normal de um sistema, serviço ou rede seja restaurada tão rapidamente quando possível e que o impacto no negócio seja minimizado;

IX - Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

X - Omissão: a não observância das políticas de segurança definidas pelo CRCMG.

CAPÍTULO II
OBJETIVO

Art. 4º A Política de Incidentes de Segurança da Informação do CRCMG tem por objetivos:

I - diminuir os danos totais causados por incidentes que não puderam ser evitados, bem como a sua reincidência;

II - promover a efetiva e eficaz Política da Segurança da Informação no CRCMG;

III - diminuir o número total de incidentes de segurança da informação envolvendo o CRCMG, por meio de prevenção sistemática dos eventos e eliminação de situações que permitam a ocorrência desses incidentes.

CAPÍTULO III
ABRANGÊNCIA

Art. 5º A Política de Incidentes de Segurança da Informação abrange todos os incidentes, confirmados ou sob suspeita, que envolvam o nome ou a propriedade do Conselho Regional de Contabilidade de Minas Gerais, bem como qualquer conselheiro, funcionário, estagiário, menor aprendiz ou colaborador, no exercício da sua função ou relação com o CRCMG.

Art. 6º A lista a seguir exemplifica, mas não esgota, os possíveis incidentes de segurança da informação tratados nesta política:

I - violar a Política de Controle de Ativos de Tecnologia da Informação do CRCMG;

II - violar uma política de segurança, explícita ou implícita;

III - realizar acesso indevido ou não autorizado a instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pelo CRCMG que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

IV - realizar acesso indevido ou não autorizado a dados, informações e documentos mantidos, tratados e controlados pelo CRCMG que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

V - conectar dispositivo de tecnologia à rede do CRCMG que esteja contaminado com vírus de computador detectado por mecanismo automatizado ou pessoal qualificado;

VI - violar norma de utilização ou configuração de dispositivo de tecnologia da informação, conectado ou não à rede do CRCMG, detectada automática ou manualmente;

VII - vazar dados pessoais;

VIII - utilizar credenciais de autenticação (senhas) por indivíduo não proprietário delas ou de outrem;

IX - facilitar fluxo de comunicação de rede caracterizado como atividade maliciosa por detecção de padrão ou análise manual, ou envolvendo dispositivos identificados por grupos de segurança como fonte de atividades maliciosas;

X - omitir a comunicação de fragilidade de segurança conhecida em processo, instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pelo CRCMG;

XI - violar direito autoral ou propriedade intelectual de qualquer natureza;

XII - realizar tentativa de fraude, bem ou malsucedida, independentemente do dano causado;

XIII - quaisquer outros eventos que constituam violação de requisito de segurança estabelecido pela Política de Segurança da Informação do CRCMG, tenham eles origem no próprio CRCMG ou em grupos externos.

CAPÍTULO IV
COMPETÊNCIAS E RESPONSABILIDADES

Seção I
COMPETÊNCIAS

Art. 7º Ao Comitê Gestor de Privacidade e Proteção de Dados compete:

I - conduzir o processo de Gestão de Incidentes de Segurança da Informação, quando se tratar de incidentes de segurança com dados pessoais, juntamente com o Comitê de Segurança da Informação e com o encarregado de dados pessoas, em conformidade com a Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCMG;

II - investigar incidentes de segurança com dados pessoais, com o levantamento da cadeia de custódia e segurança das evidências;

III - acompanhar os planos de tratamento junto aos responsáveis pelos incidentes de segurança com dados pessoais e a criação de indicadores e relatórios;

IV - realizar as análises dos pós-incidentes (post mortem) para identificação e tratamento de causas raízes e aprimoramento de processos do CRCMG e do próprio processo de gestão de incidentes de segurança com dados pessoais.

Art. 8º Ao Comitê de Segurança da Informação compete:

I - conduzir o processo de Gestão de Incidentes de Segurança da Informação e, quando se tratar de incidentes de segurança com dados pessoais, atuar juntamente com o Comitê Gestor de Privacidade e Proteção de Dados e com o encarregado de dados pessoas, em conformidade com a Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCMG;

II - executar os procedimentos de tratamento de incidentes de segurança das informações não digitais definidos nesta política no surgimento de qualquer denúncia e/ou detecção automatizada e registrar os incidentes tratados;

III - investigar incidentes de segurança da informação, com o levantamento da cadeia de custódia e segurança das evidências;

IV - comunicar aos líderes responsáveis incidentes de segurança da informação que envolvam recursos ou informações sob sua responsabilidade;

V - acompanhar os planos de tratamento junto aos responsáveis pelos incidentes e a criação de indicadores e relatórios;

VI - realizar as análises dos pós-incidentes (post mortem) para identificação e tratamento de causas raízes e aprimoramento de processos do CRCMG e do próprio processo de gestão de incidentes de segurança da informação;

VII - definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo o CRCMG;

VIII - avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos;

IX - dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

Art. 9º À Gerência de Tecnologia da Informação compete:

I - comunicar ao Comitê de Segurança da Informação e, quando aplicável, ao Comitê Gestor de Privacidade e Proteção de Dados, qualquer evento de segurança ou fragilidade sobre o qual tenha sido notificada, que possa causar prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas, serviços ou redes do CRCMG;

II - comunicar ao Comitê de Segurança da Informação e, quando aplicável, ao Comitê Gestor de Privacidade e Proteção de Dados, todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que tenha identificado ou sobre as quais tenha sido notificada, que possam indicar a possibilidade de incidentes;

III - executar os procedimentos de tratamento de incidentes de segurança da informação das informações digitais definidos nesta política, no surgimento de qualquer denúncia e/ou detecção automatizada, e registrar os incidentes tratados, conforme o modelo e operacionalização e a serem definidos em procedimento específico;

IV - definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo o CRCMG;

V - avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos;

VI - dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área;

VII - elaborar, anualmente, relatório estatístico do número de incidentes para fins de acompanhamento pelo CRCMG;

VIII - manter comunicação efetiva com o Comitê de Segurança da Informação, o Comitê Gestor de Privacidade e Proteção de Dados e o encarregado de dados pessoais sobre possíveis ameaças e ações que deverão ser adotadas para mitigação dos riscos relacionados a incidentes de segurança da informação.

Seção II
RESPONSABILIDADES

Art. 10. Os líderes, ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes pré-definidos pelo Comitê Gestor de Privacidade e Proteção de Dados e pelo Comitê de Segurança da Informação, com a devida urgência.

Art. 11. São responsabilidades de todos os conselheiros, funcionários, estagiários, menores aprendizes e colaboradores:

I - estar em capacidade de identificar incidentes de segurança da informação quando for testemunhado;

II - notificar à Gerência de Tecnologia da Informação qualquer evento de segurança ou fragilidade observada que possa causar prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas, serviços ou redes do CRCMG;

III - informar imediatamente à Gerência de Tecnologia da Informação todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

§ 1º Na apuração dos incidentes de segurança da informação, será considerada a boa ou má-fé que possa estar envolvida na realização do incidente de segurança, ou seja, o elemento subjetivo que venha a favorecer a vulnerabilidade dos dados pessoais.

§ 2º Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos conselheiros, funcionários, estagiários, menores aprendizes e colaboradores, sob o risco de violar a política de segurança digital e não digital e da informação, bem como provocar danos aos sistemas, serviços ou recursos tecnológicos digitais ou não digitais.

CAPÍTULO V
VIOLAÇÕES E SANÇÕES

Art. 12. Os conselheiros, empregados, estagiários, menores aprendizes e colaboradores que presenciarem o descumprimento de alguma das regras acima têm o dever de denunciar tal infração.

Art. 13. O descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

CAPÍTULO VI
REVISÃO E ATUALIZAÇÃO

Art. 14. A Política de Incidentes de Segurança da Informação deverá ser revista e atualizada sempre que necessário.

Art. 15. Esta resolução entra em vigor na data de sua publicação.

Aprovada na 12º Reunião Plenária, realizada em 17 de dezembro de 2021.

ROSA MARIA ABREU BARROS
Presidente do Conselho

(DOU, 05.01.2022)

BOIR6694---WIN/INTER

#IR6695#

VOLTAR

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS (CRCMG) - POLÍTICA DE NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÕES - DISPOSIÇÕES

RESOLUÇÃO CRCMG Nº 440, DE 17 DE DEZEMBRO DE 2021.

OBSERVAÇÕES INFORMEF

O Conselho Regional de Contabilidade de Minas Gerais (CRCMG), por meio da Resolução CRCMG nº 440/2021, instituiu a Política de Notificação de Incidentes der Segurança com Dados Pessoais do CRCMG, cujo objetivo é estabelecer os procedimentos necessários para a identificação, comunicação e notificação do incidente de segurança com dados pessoais.

A referida Resolução tem por finalidade descrever as medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, que os agentes de tratamento devem adotar.

Institui a Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCMG.

O CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS, no exercício de suas atribuições legais e regimentais,

Considerando a Lei nº 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

Considerando que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obrigam-se a garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o seu término;

RESOLVE:

CAPÍTULO I
POLÍTICA E DEFINIÇÕES

Art. 1º Fica instituída a Política de Notificação de Incidentes de Segurança com Dados Pessoais do Conselho Regional de Contabilidade de Minas Gerais (CRCMG).

Art. 2º Para os efeitos desta resolução, entende-se por:

I - Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso significa que um dado é considerado pessoal quando permite a identificação direta ou indireta da pessoa natural;

II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

IV - Tratamento: toda a operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transparência, difusão ou extração;

V - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No caso desta política, o CRCMG;

VI - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - Comitê Gestor de Privacidade e Proteção de Dados (CGPPD): comitê responsável pela avaliação dos mecanismos de tratamento, privacidade e proteção de dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento com vistas ao cumprimento das disposições da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito do CRCMG;

IX - Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional;

X - Notificação: ato ou efeito de informar ou de dar a conhecer sobre uma ocorrência e/ou incidente de segurança com dados pessoais.

CAPÍTULO II
OBJETIVO

Art. 3º A Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCMG tem por objetivo descrever os procedimentos necessários para a identificação, comunicação e notificação do incidente de segurança com dados pessoais.

Art. 4º Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

CAPÍTULO III
COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 5º A identificação do incidente pode ocorrer das seguintes formas:

I - denúncia por parte de titular ou terceiro;

II - reporte por parte ou operador;

III - pelo emprego de ferramentas automatizadas que detectam vazamentos de dados;

IV - através de comunicação feita por conselheiros, funcionários, estagiários, menores aprendizes e colaboradores do CRCMG, conforme disposto na Política de Incidentes de Segurança da Informação.

Art. 6º Todas as violações de dados pessoais devem ser comunicadas ao encarregado pelo tratamento de dados pessoais do CRCMG, sem demora injustificada, para registro e avaliação das medidas a serem tomadas.

Art. 7º Em caso de um incidente de segurança com dados pessoais, o operador deverá encaminhar a comunicação ao encarregado pelo tratamento de dados pessoais do CRCMG, pelo sistema disponível no portal do CRCMG, no prazo de 24 (vinte e quatro) horas, contadas da data do conhecimento do incidente.

Art. 8º No caso do titular ou terceiro, a comunicação de um incidente de segurança com dados pessoais poderá ser enviada ao encarregado pelo tratamento de dados pessoais do CRCMG, pelo sistema disponível no portal do CRCMG, preferencialmente, em até 48 (quarenta e oito) horas, contadas da data do conhecimento do incidente.

Art. 9º Na comunicação, o operador, terceiro ou titular dos dados pessoais deverá descrever sucintamente o incidente ocorrido, atentando para informações tais como:

I - descrever a natureza da violação dos dados pessoais, incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registros de dados pessoais em causa;

II - descrever as consequências prováveis da violação de dados pessoais;

III - descrever as medidas adotadas ou propostas para conduzir o caso, o que pode incluir medidas para mitigar os possíveis efeitos adversos da violação dos dados pessoais.

Art. 10. O encarregado pelo tratamento de dados pessoais do CRCMG será responsável pelo registro e análise inicial do incidente e pela resposta sobre o incidente relatado.

Art. 11. Após o registro e a análise inicial do incidente, o encarregado pelo tratamento de dados pessoais do CRCMG compartilhará a comunicação com o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) e com o Comitê de Segurança da Informação (CSI) do CRCMG, para que seja realizada a avaliação das medidas a serem tomadas.

§ 1º Caso necessário, o CGPPD ou o CSI poderá acionar a Gerência de Tecnologia da Informação (Getin) e a Assessoria Jurídica (Asjur) do CRCMG.

§ 2º O CGPPD e o CSI não realizam procedimentos de investigação criminal, e eventuais desdobramentos relacionados aos incidentes deverão ser encaminhados às autoridades policiais competentes.

Art. 12. As partes envolvidas devem seguir as orientações do encarregado pelo tratamento de dados pessoais do CRCMG, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do incidente com dados pessoais.

Art. 13. As partes envolvidas devem manter sigilo sobre a comunicação recebida, pois tornar a informação pública pode prejudicar a investigação do suposto incidente com dados pessoais e a identificação do autor do incidente.

CAPÍTULO IV
NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 14. O CRCMG notificará a ANPD e o titular da ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares.

§ 1º O CRCMG deverá avaliar internamente a relevância do risco ou dano do incidente de segurança para determinar se deverá comunicar à ANPD e ao titular.

§ 2º Para a avaliação interna, deverão ser analisados os incidentes que envolvam especialmente:

I - dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou que tenham o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade;

II - volume de dados envolvidos, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

§ 3º A notificação não será necessária se o responsável pelo tratamento puder demonstrar, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

Art. 15. Caso necessária, a notificação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Art. 16. Caso não seja possível fornecer todas as informações no momento da notificação preliminar, informações adicionais poderão ser fornecidas posteriormente, sendo que, no momento da notificação preliminar, deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las.

Art. 17. A notificação à ANPD será feita por intermédio do encarregado pelo tratamento de dados pessoais do CRCMG.

Parágrafo único. O encarregado pelo tratamento de dados pessoais do CRCMG comunicará o incidente com dados pessoais à ANPD, com base nas análises técnicas e jurídicas realizadas pelo CGPPD, pelo CSI, pela Getin e pela Asjur do CRCMG.

Art. 18. O encarregado pelo tratamento de dados pessoais do CRCMG ainda tem como responsabilidade:

I - aprovar e autorizar a divulgação de comunicado aos titulares envolvidos no incidente com dados pessoais;

II - validar quaisquer comunicados ao público, imprensa e usuários referentes ao incidente com dados pessoais;

III - orientar e/ou informar as equipes interessadas a respeito das práticas a serem adotadas com relação ao incidente com dados pessoais;

IV - coordenar todas as ações decorrentes do incidente com dados, com o intuito de mitigar os impactos percebidos;

V - atuar como porta-voz do CRCMG perante a ANPD, demais autoridades competentes e os usuários, supervisionando os contatos e comunicações com o público, decorrentes do incidente com dados pessoais, dentre outras atividades.

Art. 19. Esta resolução entra em vigor na data da sua publicação.

Aprovada na 12º Reunião Plenária, realizada em 17 de dezembro de 2021.

ROSA MARIA ABREU BARROS
Presidente do Conselho

(DOU, 05.01.2022)

BOIR6695---WIN/INTER

#IR6646#

VOLTAR

DECISÕES ADMINISTRATIVAS DA RECEITA FEDERAL DO BRASIL

IR - PESSOA JURÍDICA - CSLL - INCENTIVOS FISCAIS - INCENTIVOS E BENEFÍCIOS FISCAIS OU FINANCEIROS-FISCAIS RELATIVOS AO ICMS - SUBVENÇÃO PARA INVESTIMENTO - REQUISITOS E CONDIÇÕES - AUSÊNCIA

SOLUÇÃO DE CONSULTA Nº 99.010, DE 9 DE NOVEMBRO DE 2021

ASSUNTO: IMPOSTO SOBRE A RENDA DE PESSOA JURÍDICA - IRPJ

INCENTIVOS FISCAIS. INCENTIVOS E BENEFÍCIOS FISCAIS OU FINANCEIROS-FISCAIS RELATIVOS AO ICMS. SUBVENÇÃO PARA INVESTIMENTO. REQUISITOS E CONDIÇÕES. AUSÊNCIA.

A partir da Lei Complementar nº 160, de 2017, os incentivos e os benefícios fiscais ou financeiro-fiscais relativos ao ICMS, concedidos por estados e Distrito Federal e considerados subvenções para investimento por força do § 4º do art. 30 da Lei nº 12.973, de 2014, poderão deixar de ser computados na determinação do lucro real desde que observados os requisitos e as condições impostos pelo art. 30 da Lei nº 12.973, de 2014, dentre os quais, a necessidade de que tenham sido concedidos como estímulo à implantação ou expansão de empreendimentos econômicos.

SOLUÇÃO DE CONSULTA VINCULADA À SOLUÇÃO DE CONSULTA COSIT Nº 145, DE 15 DE DEZEMBRO DE 2020.

DISPOSITIVOS LEGAIS: *Lei nº 12.973, de 2014, art. 30; Lei Complementar nº 160, de 2017, arts. 9º e 10; Parecer Normativo Cosit nº 112, de 1978; Instrução Normativa RFB nº 1.700, de 2017, art. 198.*

ASSUNTO: CONTRIBUIÇÃO SOCIAL SOBRE O LUCRO LÍQUIDO - CSLL

INCENTIVOS FISCAIS. INCENTIVOS E BENEFÍCIOS FISCAIS OU FINANCEIROS-FISCAIS RELATIVOS AO ICMS. SUBVENÇÃO PARA INVESTIMENTO. REQUISITOS E CONDIÇÕES. AUSÊNCIA.

A partir da Lei Complementar nº 160, de 2017, os incentivos e os benefícios fiscais ou financeiro-fiscais relativos ao ICMS, concedidos por estados e Distrito Federal e considerados subvenções para investimento por força do § 4º do art. 30 da Lei nº 12.973, de 2014, poderão deixar de ser computados na determinação do

resultado ajustado desde que observados os requisitos e as condições impostos pelo art. 30 da Lei nº 12.973, de 2014, dentre os quais, a necessidade de que tenham sido concedidos como estímulo à implantação ou expansão de empreendimentos econômicos.

SOLUÇÃO DE CONSULTA VINCULADA À SOLUÇÃO DE CONSULTA COSIT Nº 145, DE 15 DE DEZEMBRO DE 2020.

DISPOSITIVOS LEGAIS: *Lei nº 12.973, de 2014, arts. 30 e 50; Lei Complementar nº 160, de 2017, arts. 9º e 10; Parecer Normativo Cosit nº 112, de 1978; Instrução Normativa RFB nº 1.700, de 2017, art. 198.*

FÁBIO CEMBRANEL
Coordenador da Cotir

(DOU, 16.11.2021)

BOIR6646---WIN/INTER

#IR6677#

VOLTAR

GÁS NATURAL - FONTE DE ENERGIA - VENDA PARA PESSOA JURÍDICA PREPONDERANTEMENTE EXPORTADORA - SUSPENSÃO - INAPLICABILIDADE - CONTRIBUIÇÃO PARA O FINANCIAMENTO DA SEGURIDADE SOCIAL - COFINS

SOLUÇÃO DE CONSULTA Nº 186, DE 13 DE DEZEMBRO DE 2021

ASSUNTO: CONTRIBUIÇÃO PARA O FINANCIAMENTO DA SEGURIDADE SOCIAL - COFINS

GÁS NATURAL. FONTE DE ENERGIA. VENDA PARA PESSOA JURÍDICA PREPONDERANTEMENTE EXPORTADORA. SUSPENSÃO. INAPLICABILIDADE.

O gás natural comercializado para ser utilizado como fonte de energia e calor em máquinas e equipamentos industriais não constitui produto intermediário incorporado ao produto final. Consequentemente, fica vedada a aplicação do benefício da suspensão da incidência da Cofins de que trata o art. 40 da Lei nº 10.865, de 2004, sobre as receitas auferidas por pessoa jurídica que executa atividades de distribuição e de seu fornecimento à pessoa jurídica preponderantemente exportadora.

SOLUÇÃO DE CONSULTA PARCIALMENTE VINCULADA À SOLUÇÃO DE DIVERGÊNCIA COSIT Nº 37, DE 09 DE OUTUBRO DE 2008; E À SOLUÇÃO DE CONSULTA COSIT Nº 301, DE 14 DE JUNHO DE 2017.

DISPOSITIVOS LEGAIS: *Art. 40 da Lei nº 10.865, de 2004, e art. 548 da Instrução Normativa RFB nº 1.911, de 2019.*

ASSUNTO: CONTRIBUIÇÃO PARA O PIS/PASEP

GÁS NATURAL. FONTE DE ENERGIA. VENDA PARA PESSOA JURÍDICA PREPONDERANTEMENTE EXPORTADORA. SUSPENSÃO. INAPLICABILIDADE.

O gás natural comercializado para ser utilizado como fonte de energia e calor em máquinas e equipamentos industriais não constitui produto intermediário incorporado ao produto final. Consequentemente, fica vedada a aplicação do benefício da suspensão da incidência da Contribuição para o PIS/Pasep de que trata o art. 40 da Lei nº 10.865, de 2004, sobre as receitas auferidas por pessoa jurídica que executa atividades de distribuição e de seu fornecimento à pessoa jurídica preponderantemente exportadora.

SOLUÇÃO DE CONSULTA PARCIALMENTE VINCULADA À SOLUÇÃO DE DIVERGÊNCIA COSIT Nº 37, DE 09 DE OUTUBRO DE 2008; E À SOLUÇÃO DE CONSULTA COSIT Nº 301, DE 14 DE JUNHO DE 2017.

DISPOSITIVOS LEGAIS: *Art. 40 da Lei nº 10.865, de 2004, e art. 548 da Instrução Normativa RFB nº 1.911, de 2019.*

FERNANDO MOMBELLI
Coordenador-Geral

(DOU, 16.12.2021)

BOIR6677---WIN/INTER