

BOLETIM



GESTÃO DE PESSOAS & RECURSOS HUMANOS

IPEA, 21 de MAIO de 2014 - EXTRA Nº 05

INSTITUTO DE PESQUISA ECONÔMICA APLICADA

PORTARIA nº 078, DE 20 DE MAIO DE 2014.

Institui a sala de pesquisa em dados sigilosos no Ipea e os procedimentos necessários para tratamento de informações sigilosas.

O PRESIDENTE SUBSTITUTO DO INSTITUTO DE PESQUISA ECONÔMICA APLICADA - Ipea, no uso de suas atribuições que lhe são conferidas pelo art. 17, do Decreto nº 7.142, de 29 de março de 2010, publicado no D.O.U de 30 de março de 2010, e considerando a Lei nº 12.527, de 18 de novembro de 2011, o Decreto nº 7.845, de 14 de novembro de 2012, a Portaria Ipea nº 324, de 21 de julho de 2010, a Portaria Ipea nº 426, de 10 de novembro de 2010, e a Portaria Ipea nº 456, de 2 de dezembro de 2010, resolve:

Art. 1º. Instituir, na forma desta portaria, a sala de pesquisa em dados sigilosos do Ipea, doravante denominada “Sala de Sigilo”.

§ 1º Esta portaria complementa os Incisos I, VI e VII do Art. 7º da Política de Segurança da Informação e Comunicações – POSIC, estabelecida pela Portaria Ipea nº 456, de 2 de dezembro de 2010.

§ 2º Esta portaria regulamenta no âmbito do Ipea os procedimentos de segurança, custódia e tratamento de dados e informações destinadas ao uso em projetos de pesquisa e assessoramento técnico ao Estado brasileiro, classificadas em qualquer grau de sigilo, nos termos dos Artigos 46 e 57 do Decreto número 7.845, de 14 de novembro de 2012.

§ 3º A sala de sigilo do Ipea é um ambiente seguro para disponibilização de ferramentas de pesquisa e análise para uso exclusivo de interesse institucional do Ipea e do Estado brasileiro.

CAPÍTULO I – DO OBJETIVO E CAMPO DE APLICAÇÃO

Art. 2º. A sala de sigilo do Ipea tem como objetivos:

- I - Proteção da informação sigilosa e da informação pessoal disponibilizada ao Ipea por outros órgãos de governo, observada a sua disponibilidade, autenticidade,

integridade e eventual restrição de acesso, nos termos da Lei nº 12.527, de 18 de novembro de 2011, da Lei Complementar Nº 105, de 10 de janeiro de 2001 e das legislações específicas que regem o acesso às informações sigilosas sob a guarda do Estado; e

II - Permitir acesso controlado e restrito a bases de dados sigilosas, por meio de um conjunto de protocolos e ferramentas que garantam processos seguros de utilização e sigilo.

Art. 3º Somente poderão ter acesso e utilizar a sala de sigilo do Ipea:

I - Os integrantes das equipes técnicas de pré-processamento, dos grupos de avaliação de extração de resultados e equipe de segurança da CGTIC previstos nos incisos X e XI do art. 4º e no inciso I do Art. 14º;

II - Demais servidores, bolsistas, consultores e colaboradores do Ipea trabalhando na produção de pesquisas de interesse da Instituição, quando devida e formalmente autorizados pelo diretor ou assessor chefe da área a qual estão vinculados; e

III - Servidores públicos externos ao Ipea que estejam trabalhando na produção de pesquisas de interesse do Estado, quando devida e formalmente autorizados pelo Presidente, diretor ou assessor chefe no Ipea.

CAPÍTULO II – DOS TERMOS E DEFINIÇÕES

Art. 4º - Para efeitos desta Portaria, ficam estabelecidos os seguintes termos e definições, em complemento à Política de Segurança da Informação e Comunicações do Ipea:

I - Bases de Dados: conjunto de dados interrelacionados, organizados de forma a permitir a recuperação da informação;

II - Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem clara por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

III - Controles Físicos de Segurança: são barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura (que garante a existência da informação) que a suporta;

IV - Controles Lógicos de Segurança: são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a quebra de confidencialidade e de integridade;

V - Informação Pessoal: aquela relacionada à pessoa natural identificada ou identificável, conforme estabelecido na Lei Nº 12.527, de 18 de novembro de 2011;

VI - Informação Pública: aquela que não permite a identificação pessoal, de pessoa jurídica ou local individualizado e que está disponível ao público em geral;

VII - Informação Restrita: aquela que não é pública e cujo acesso requer algum nível de controle e de autorização prévia;

VIII - Informação Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, nos termos do Art. 23 da Lei Nº 12.527, de 18 de novembro de 2011 ou de legislação específica;

- IX - Tratamento da Informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação, conforme estabelecido na Lei Nº 12.527, de 18 de novembro de 2011;
- X - Equipes Técnicas de pré-processamento: equipes formadas por servidores da ASTEC, da CGTIC, e/ou de diretorias relacionadas, que serão responsáveis pela inserção, manutenção e atualização de bases de dados nos computadores e nos servidores da sala de sigilo.
- XI - Grupos de Avaliação de Extração de Resultados: grupos compostos por um servidor indicado pela ASTEC e no mínimo mais um indicado pelas diretorias relacionadas com a pesquisa, cuja função será a avaliação de resultados e de códigos computacionais, a fim de garantir que os resultados preservem o sigilo das informações individuais.

CAPÍTULO III – DO MODELO DE IMPLANTAÇÃO E FUNCIONAMENTO

Art. 5º - Os dados disponibilizados na sala de sigilo do Ipea estão divididos em três categorias, para efeito de controle de acesso:

- I - Bases de dados públicas: são aquelas contendo informações públicas, às quais não é necessária a aplicação de controles de acesso;
- II - Bases de dados restritas: são aquelas contendo informações restritas, cujo acesso requer autorização prévia da unidade gestora das bases de dado no Ipea e às quais devem ser aplicados controles lógicos de segurança;
- III - Base de dados sigilosa: são aquelas contendo informação sigilosa ou pessoal, cujo acesso requer autorização específica da unidade gestora da base de dado no Ipea e/ou do cedente e às quais devem ser aplicados controles lógicos e físicos de segurança;

Parágrafo único: os controles de acesso poderão permitir o acesso simultâneo a mais de uma base de dados, desde que as condições de restrição e de controle de acesso de cada uma das bases sejam respeitadas.

Art. 6º - O acesso às informações na Sala de Sigilo do Ipea deverá ser feito com ciência prévia da ASTEC, mediante autorização da diretoria ou assessoria a qual a pesquisa está relacionada.

§ 1º A solicitação de uso da sala deverá ser feita por servidor do Ipea, por meio de formulário específico, conforme o modelo do Anexo I desta portaria e aprovada pela diretoria ou assessoria a qual a pesquisa está relacionada;

Art. 7º - O acesso às informações disponíveis na sala de sigilo do Ipea deverá respeitar controles físicos e lógicos.

§ 1º Somente pessoas autorizadas nos termos do art. 3º podem ter acesso às instalações e equipamentos localizados na sala de sigilo;

§ 2º O acesso à sala de sigilo exigirá identificação e registro biométrico dos usuários;

§ 3º A disponibilização da infraestrutura computacional na sala de sigilo deverá respeitar os seguintes controles físicos:

- I - Os computadores deverão estar fisicamente isolados de outras redes de computadores e equipamentos externos à sala de sigilo;
- II - Os equipamentos servidores, ativos de rede e sistemas de armazenamento centralizado de dados deverão ser mantidos em gabinetes com trava de segurança, que dificulte o acesso direto ao equipamento, e com portas de comunicação e dispositivos que permitam a leitura, a gravação e a comunicação de dados por profissionais autorizados;
- III - O acesso físico direto aos equipamentos e mecanismos de controle físico previstos no Inciso anterior somente poderá ser feito com autorização da ASTEC;
- IV - Nenhum dispositivo de gravação poderá ser conectado à infraestrutura computacional na sala de sigilo, sem autorização prévia da ASTEC e da CGTIC conforme modelo do Anexo IV;
- V - Nenhum dispositivo de armazenamento contendo ou que conteve dados sigilosos poderá ser retirado da sala sem o devido saneamento/exclusão de todos os dados, ou a inutilização do dispositivo;

§ 4º A disponibilização de informações na sala de sigilo deverá respeitar os seguintes controles lógicos:

- I - Identificação lógica única e intransferível de cada usuário, por meio de certificação digital ou senhas pessoais ou mecanismos biométricos, ou outras ferramentas de segurança tecnologicamente iguais ou superiores;
- II - Segregação de permissões de acesso, por base de dados, conforme classificação prevista no Art. 5º desta norma;
- III - Registro eletrônico de acesso lógico aos equipamentos e bases de dados para fins de auditoria;
- IV - Cifração dos dados quando for tecnicamente viável e quando não acarretar prejuízo aos procedimentos lícitos de pesquisa.

§ 5º A sala de sigilo deverá ser monitorada em tempo integral, sem prejuízo à confidencialidade das informações armazenadas nela, por dispositivos de vigilância eletrônica que deverá registrar em vídeo os acessos e as atividades internas e imediatamente externas ao ambiente;

§ 6º É vedada a entrada de aparelhos eletrônicos na sala de sigilo, com exceção dos dispositivos para manutenção de equipamentos e para a carga e a extração de dados autorizados.

Art. 8º - A entrada de dados na sala de sigilo do Ipea deverá respeitar procedimentos, protocolos e controles físicos e lógicos.

§ 1º A preparação, carga e atualização dos dados serão executados pela equipe técnica de pré-processamento.

§ 2º Toda entrada de dados deverá ser registrada em sistema eletrônico.

§ 3º Os dispositivos de armazenamento usados para transferência de informação sigilosa deverão ser devolvidos à cedente, mantidos na sala de sigilo ou destruídos.

§ 4º Os protocolos e procedimentos para entrada de dados serão estabelecidos em ato conjunto da ASTEC e da CGTIC.

Art. 9º - A saída de informações da sala de sigilo do Ipea deverá respeitar procedimentos, protocolos e controles físicos e lógicos.

§ 1º Uma vez efetuadas as análises, os usuários deverão preencher o formulário contido no Anexo II desta portaria, solicitando a extração das informações;

§ 2º As solicitações de extração de informações serão recebidas pela ASTEC e encaminhadas ao grupo de avaliação de extração de resultados;

§ 3º Para a extração de tabulações deve ser avaliado se o produto elaborado atende às exigências quanto à preservação do sigilo estatístico das informações;

§ 4º Em tabelas de frequência não serão disponibilizadas informações para células com menos de três registros;

§ 5º Tanto os arquivos gerados quando a programação utilizada para o seu processamento deverão ser armazenados para análise e auditoria;

§ 6º Uma vez aprovados, os arquivos gerados poderão ser extraídos da sala e enviados por e-mail aos usuários, pela ASTEC, mantendo-se cópia e registro dos arquivos retirados.

Art. 10 - O acesso à sala de sigilo do Ipea para limpeza e manutenção deverá respeitar os seguintes procedimentos:

- I - O acesso à sala deve ser registrado e acompanhado pela ASTEC;
- II - No caso de manutenção dos equipamentos, o acesso aos mesmos e a execução dos serviços deverão ser acompanhados pela equipe de segurança da informação da CGTIC; e
- III - Dispositivos defeituosos de armazenamento físico de dados somente poderão ser substituídos mediante sua inutilização ou retenção pelo Ipea.

Art. 11 - Todos os usuários, membros das equipes técnicas, de administração, de manutenção e de segurança que tenham acesso à sala deverão assinar o termo de sigilo do Anexo III desta norma.

CAPÍTULO IV – DAS RESPONSABILIDADES

Art. 12 - Cabe à Assessoria Técnica da Presidência – ASTEC:

- I - Gestão da sala de sigilo do Ipea;
- II - Manter controle das autorizações recebidas das diretorias e dos acessos à sala de sigilo;
- III - Manter em pleno funcionamento e operação a infraestrutura física da sala de sigilo;
- IV - Acompanhar serviços de entrada e saída de dados e de manutenção do ambiente;
- V - Gravar as análises aprovadas e enviar aos usuários.

Art. 13 - Cabe às Diretorias do Ipea:

- I - Designar servidores e colaboradores dos seus quadros para execução de tarefas específicas de operação e gestão da sala de sigilo, o que inclui participação nos grupos de avaliação de extração de resultados; e
- II - Autorizar o acesso à sala de sigilo do pessoal descrito no art. 3º desta portaria em pesquisas a elas relacionadas;

Art. 14 - Cabe à Coordenação Geral de Tecnologia da Informação e Comunicação - CGTIC:

- I - Manter equipe de segurança para atuar em tarefas específicas da operação, gestão e auditoria da sala de sigilo;
- II - Instalar e manter a infraestrutura computacional da sala de sigilo;
- III - Propor, implantar e manter os controles lógicos da sala de sigilo; e
- IV - Gerar e manter cópias de segurança previstas nesta norma;
- V - Definir e implantar mecanismos criptográficos para a cifração de dados, quando necessário.

Art. 15 - Cabe às equipes técnicas de pré-processamento: atualizar e manter bases existentes, e processar, limpar e verificar novas bases de dados inseridas na sala de sigilo.

Art. 16 - Cabe aos grupos de avaliação de extração de resultados: verificar e aprovar a extração solicitada pelos usuários da sala de sigilo, nos termos desta norma.

Art. 17 - Cabe aos usuários da sala de sigilo: respeitar os protocolos e procedimentos previstos nesta norma.

Art. 18 Casos omissos relativos à segurança da informação serão resolvidos pelo Gestor de Segurança da Informação e Comunicações do Ipea, nos termos do Art. 4º da Portaria Nº 321 de 21 de julho de 2010;

Art. 19 Casos omissos relativos à gestão e operação da sala de sigilo serão resolvidos pela Assessoria Técnica da Presidência – ASTEC.

Art. 20 O resultado das pesquisas será sempre público e acessível a todo cidadão, salvo aquele em que o órgão requisitante impuser alguma restrição em sua divulgação ou seja sigiloso por sua natureza.

Art. 21. Esta Portaria entra em vigor na data de sua publicação.

SERGEI SUAREZ DILLON SOARES

Autorização para acesso à Sala de Sigilo e pelo uso da informação

Data de liberação do acesso: ___/___/___

Data de expiração do acesso: ___/___/___

Diretor Responsável

Nome legível

Assinatura

Controle da Assessoria Técnica da Presidência – ASTEC

Nome legível

Assinatura

ANEXO II

TERMO DE SOLICITAÇÃO DE RETIRADA DE INFORMAÇÕES DA SALA DE SIGILO

Identificação do solicitante

Nome do Pesquisador/Colaborador:		
CPF:		Matrícula SIAPE:
Login:	E-mail:	Telefone/Ramal:
Diretoria:		
Título da Pesquisa:		

Descrição das Informações para Retirada

Número do computador utilizado:
Diretório contendo os arquivos gerados:
Bases de dados utilizadas:
Softwares utilizados:
Descrição das atividades efetuadas:
Conteúdo das informações geradas para extração da sala de sigilo:

Relatório do Grupo de Avaliação de Extração de Resultados

Resultado da avaliação: () Aprovamos a retirada das informações
() Não aprovamos a retirada das informações
() Aprovamos a retirada com modificações

Recomendações e/ou comentários adicionais:

Data de avaliação das informações geradas: __/__/____

Identificação do primeiro avaliador

Nome legível

Assinatura

Identificação do segundo avaliador

Nome legível

Assinatura

Para uso da ASTEC

Autorização para retirada das informações da Sala de Sigilo

Data de liberação da retirada: __/__/____

Assessoria Técnica da Presidência – ASTEC

Nome legível

Assinatura

ANEXO III

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - TCMS

[Qualificação: nome, nacionalidade, CPF, identidade (no, data e local de expedição), filiação e endereço], perante o Instituto de Pesquisa Econômica Aplicada - Ipea, declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e a:

- a) assumir inteira responsabilidade sobre o uso da informação disponibilizada nesta Sala de Sigilo, em conformidade com as normas estabelecidas pela Portaria nº ____/2014 e outras que regulam o assunto denominado pelo Ipea como “bases de dados estatísticos”;
- b) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo Ipea e preservar o seu sigilo, de acordo com a legislação vigente;
- c) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;
- d) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito;
- e) não copiar ou reproduzir, por qualquer meio ou modo: (i) informações classificadas em qualquer grau de sigilo; (ii) informações relativas aos materiais de acesso restrito disponibilizado pelo Ipea, salvo autorização da autoridade competente;

Firmo ainda o compromisso de utilizá-las apenas para estudos e pesquisas desenvolvidos para o Ipea, me comprometendo sempre a divulgar a(s) respectiva(s) fonte(s) produtora(s) dos dados no(s) trabalho(s) dela(s) resultante(s).

Declaro que recebi acesso à sala de sigilo do Ipea e dos dados nela contidos, e por estar de acordo com o presente Termo, o assino na presença das testemunhas abaixo identificadas.

[Local e data]

Assinatura

Nome legível e assinatura do Diretor da Área

[Nome 1ª Testemunha]
Identidade
CPF

[Nome 1ª Testemunha]
Identidade
CPF

ANEXO IV

TERMO DE AUTORIZAÇÃO PARA USO DE DISPOSITIVOS DE GRAVAÇÃO

Identificação do responsável pelo uso do dispositivo

Nome do Responsável:

Matrícula SIAPE:

Justificativa

Autorização

Data: __/__/__

Assessoria Técnica da Presidência – ASTEC

Nome legível

Assinatura

Coordenação Geral de Tecnologia da Informação e Comunicação - CGTIC

Nome legível

Assinatura