CONTROLADORIA-GERAL DA UNIÃO

NOTA TÉCNICA Nº 1176/2021/CGUNE/CRG

PROCESSO Nº 00190.112020/2019-51

INTERESSADO: MINISTÉRIO DA ECONOMIA

1. ASSUNTO

1.1. Videoconferência. Tratamento da informação em ambiente de computação em nuvem.

1.2. Instrução Normativa nº.12, de 1º de novembro de 2011, DOU de 03 de novembro de 2011, Seção 1, p.26;

1.3. Instrução Normativa nº.14, de 14 de novembro de 2018, DOU de 16 de novembro de 2018, Seção 1, p.102;

1.4. Instrução Normativa nº.05, de 21 de fevereiro de 2020, DOU de 26 de fevereiro de 2020, Seção 1, p.156;

1.5. Lei nº.13.709, de 14 de agosto de 2018, DOU de 15 de agosto de 2018;

1.6. Norma Complementar nº.14/IN01/DSIC/SCS/GSIPR, de 13 de março de 2018;

1.7. Lei nº.12.527, de 18 de novembro de 2011, DOU de 18 de novembro de 2011;

1.8. Orientação Conjunta nº 1//2021/ME/CGU, de 12 de março de 2021.

2. ANÁLISE

2.1. Trata-se de processo autuado a partir do recebimento do Ofício SEI nº. 93101/2019/ME, de 12 de dezembro de 2019, da Sra. Corregedora-Geral do Ministério da Economia, com o seguinte teor:

> *Cumprimentando-o, cordialmente, submeto à sua análise os seguintes considerandos e questões:*
>
> *1. Considerando o avanço das ferramentas tecnológicas de reunião online disponíveis e as vantagens associadas;*
>
> *2. Considerando a necessidade de aumento na produtividade e celeridade das atividades correcionais para uma maior efetividade;*
>
> *3. Considerando a necessidade de racionalização de uso dos recursos públicos evitando viagens e hospedagens de membros e interessados nos processos correcionais;*
>
> *4. Que esta Corregedoria-Geral pretende implementar o uso sistemático da ferramenta Microsoft Teams;*
>
> *Quais as recomendações gerais administrativas e normativas dessa CGU para uso de ferramentas dessa natureza (videoconferência através de serviços de nuvem)? Quais as restrições administrativas e normativas dessa CGU ao uso de ferramentas online para consecução de oitivas de acusados, testemunhas e informantes por videoconferência?*

2.2. A Corregedoria-Geral do Ministério da Economia indaga ao Órgão

Central quais as recomendações administrativas e normativas para o uso de ferramentas *online* para realização de oitivas de acusados, testemunhas e informantes por videoconferência através de serviços de nuvem.

2.3. A Corregedoria-Geral da União, no exercício das funções de órgão central do Sistema de Correição do Poder Executivo Federal, editou a Instrução Normativa nº.12, de 1º de novembro de 2011, publicada no Diário Oficial da União de 03 de novembro de 2011, Seção 1, p.26, para regulamentar a adoção de videoconferência na instrução de processos e procedimentos disciplinares no âmbito do Sistema de Correição do Poder Executivo Federal (SISCOR). Transcreve-se abaixo o inteiro teor da norma, em sua redação original:

> *IN 12/2011 (redação original)*
>
> *Art. 1º. O Sistema de Correição do Poder Executivo Federal - SisCor-PEF, visando instrumentalizar a realização de atos processuais a distância, poderá promover a tomada de depoimentos, acareações, investigações e diligências por meio de videoconferência ou outro recurso tecnológico de transmissão de sons e imagens em tempo real, assegurados os direitos ao contraditório e à ampla defesa, na forma disciplinada nesta Instrução Normativa.*
>
> *Parágrafo único. Nos termos dos artigos 153 e 155 da Lei 8.112/90, os meios e recursos admitidos em direito e previstos no caput serão utilizados no intuito de garantir a adequada produção de provas, de modo a permitir a busca da verdade real dos fatos, visando, em especial, à proteção dos direitos dos administrados e ao melhor cumprimento dos fins da Administração.*
>
> *Art. 2º Poderão ser realizadas audiências e reuniões por meio de teletransmissão de sons e imagens ao vivo e em tempo real, destinadas a garantir a adequada produção da prova, sem prejuízo de seu caráter reservado, nos procedimentos de natureza disciplinar ou investigativa.*
>
> *Art. 3º. Nos processos administrativos disciplinares, a decisão da Comissão Disciplinar pela realização de audiência por meio de videoconferência deverá, de maneira motivada:*
>
> *I - assegurar a todos a razoável duração do processo e os meios que garantam a celeridade de sua tramitação e;*
>
> *II - viabilizar a participação do servidor investigado, testemunha, técnico ou perito, quando os mesmos residirem em local diverso da sede dos trabalhos da Comissão Disciplinar. Parágrafo único. As reuniões e as audiências das comissões terão caráter reservado.*
>
> *Art. 4º. O Presidente da Comissão Disciplinar notificará a pessoa a ser ouvida da data, horário e local em que será realizada a audiência ou reunião por meio de videoconferência, com antecedência mínima de 10 (dez) dias.*
>
> *§ 1º Em qualquer caso, a defesa será notificada, nos termos do caput, para acompanhar a realização do ato.*
>
> *§ 2º Ao deliberar pelo horário da realização da audiência por meio de videoconferência, a Comissão Disciplinar atentará para eventual diferença de fuso horário entre as localidades envolvidas.*
>
> *Art. 5º. Ao servidor investigado e seu procurador é facultado acompanhar a audiência ou reunião realizada por videoconferência:*
>
> *I - na sala em que se encontrar a Comissão Disciplinar;*
>
> *ou II - na sala em que comparecer a pessoa a ser ouvida.*
>
> *Parágrafo único. Em casos excepcionais, a Comissão Disciplinar decidirá acerca do comparecimento dos envolvidos em local diverso dos estabelecidos nos incisos deste artigo.*
>
> *Art. 6º. A Comissão Disciplinar solicitará ao responsável pela unidade envolvida a designação de servidor para o exercício da função de secretário ad hoc.*
>
> *§ 1º O secretário ad hoc desempenhará atividades de apoio aos trabalhos da Comissão Disciplinar, tais como identificação dos participantes do ato,*

encaminhamento e recebimento de documentos, extração de cópias, colheita de assinaturas, dentre outras determinadas pelo Presidente da Comissão Disciplinar.

§ 2º. Cabe, ainda, ao secretário ad hoc acompanhar os testes de equipamento e conexões antes da realização do ato, devendo comunicar imediatamente à Comissão Disciplinar acerca de eventual circunstância que impossibilite seu uso.

Art. 7º. O depoimento prestado pelas partes será reduzido a termo, mediante lavratura do termo de depoimento, a ser realizado por membro da Comissão Disciplinar ou pelo secretário participante.

Parágrafo único. O termo de depoimento será assinado, nas diversas localidades, pelos participantes do ato e posteriormente juntado aos autos do processo.

Art. 8º. Todas as formalidades necessárias para a concretização dos atos instrutórios observarão, no que couber, o disposto na Lei n° 8.112, de 11 de dezembro de 1990, e, subsidiariamente, na Lei n° 9.784, de 29 de janeiro de 1999, devendo as questões de ordem ser dirimidas pelo Presidente da Comissão ou responsável pela condução do processo.

Art. 9º. Esta Instrução Normativa entra em vigor na data de sua publicação.

2.4. Por sua vez, a Instrução Normativa nº.14, de 14 de novembro de 2018, publicada no Diário Oficial da União de 16 de novembro de 2018, Seção 1, p.102, a qual regulamenta a atividade correcional no âmbito do SISCOR, estabeleceu o uso preferencial da videoconferência para tomada de depoimentos no âmbito do processo administrativo disciplinar, conforme artigo 33, §11:

IN 14/2018

Art. 33. O PAD será instaurado e conduzido nos termos da Lei nº 8.112, de 1990.

(...)

§ 11. A tomada de depoimentos de pessoas que se encontrem em localidade distinta da comissão será realizada, preferencialmente, por meio de videoconferência.

2.5. Posteriormente, o referido normativo foi alterado pela Instrução Normativa nº.05, de 21 de fevereiro de 2020, publicada no Diário Oficial da União de 26 de fevereiro de 2020, Seção 1, p.156, a qual explicitou a desnecessidade de transcrição em ata do teor das audiências realizadas por meio de videoconferência bem como da aposição de assinatura dos participantes no referido documento, *in verbis*:

IN 05/2020

"Art. 6º A Comissão Disciplinar poderá solicitar ao responsável pela unidade envolvida a designação de servidor para o exercício da função de secretário ad hoc.

§ 1º .....

§ 2 .....

"Art. 7º O registro audiovisual gerado em audiência deverá ser juntado aos autos, sem necessidade de transcrição em ata, sendo disponibilizado à defesa o acesso ao seu conteúdo ou à respectiva cópia.

§ 1º O presidente da Comissão Disciplinar assinará a ata de audiência lavrada, na qual serão registrados, pelo menos, a data, os locais e os participantes do ato.

§ 2º O registro nominal e individualizado da presença de cada um dos participantes na gravação dispensa as suas assinaturas na ata de audiência."

2.6. Por último, há de se mencionar ainda a edição da Instrução Normativa nº.09, de 24 de março de 2020, publicada no Diário Oficial da União de 26 de março de 2020, Seção 1, p.128, que faculta a realização de qualquer ato de comunicação processual - inclusive notificação prévia, intimação de testemunha ou declarante, intimação de investigado ou acusado, intimação para apresentação de alegações escritas e alegações finais, e citação para apresentação de defesa escrita - por meio de correio eletrônico institucional, aplicativos de mensagens instantâneas ou recursos tecnológicos similares.

2.7. Depreende-se de todo o arcabouço normativo apresentado que a condução dos processos de responsabilização disciplinar por meio de ferramentas tecnológicas, que substituem a presença física simultânea dos integrantes da Comissão, acusados, testemunhas, advogados e demais participantes dos atos administrativos, está devidamente amparada em normativos e representa cada vez mais a realidade de trabalho das unidades correcionais.

2.8. Com os avanços tecnológicos, a exemplo do armazenamento de dados em nuvem, e o permanente incremento na utilização de tais ferramentas tecnológicas, surgem também questionamentos acerca da segurança no tocante ao armazenamento de dados e à transmissão fidedigna das informações, preocupação esta realçada com a vigência da Lei Geral de Proteção de Dados (Lei nº.13.709, de 14 de agosto de 2018), que impõe que todo tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, deve proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.9. Em consulta à Diretoria de Tecnologia de Informação desta CGU, apontou-se a necessidade de observância do teor da Norma Complementar nº.14/IN01/DSIC/SCS/GSIPR, de 13 de março de 2018, editada pelo Departamento de Segurança da Informação e Comunicações da Secretaria de Coordenação de Sistemas do Gabinete de Segurança Institucional da Presidência da República, a qual estabelece os Princípios, Diretrizes e Responsabilidades relacionados à Segurança da Informação para o tratamento da informação em ambiente de computação de nuvem (1953292).

2.10. A referida Norma Complementar tem como objetivo *"estabelecer princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da Informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta".*

2.11. A norma define o termo Computação em Nuvem como o *"modelo computacional que permite acesso por demanda, e independentemente de localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), supervisionados com esforços mínimos de gestão ou interação com o provedor de serviços."*. Por sua vez, tratamento de informação é *"o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.".*

2.12. O item 5.1 da Norma estabelece que o tratamento de informação em ambiente de computação em nuvem deve observar, no mínimo, as seguintes diretrizes:

> *5.1.1. A prevalência dos direitos e garantias fundamentais no tratamento das informações pessoais;*
>
> *5.1.2 As diretrizes estabelecidas em sua Política de Segurança de Informação e Comunicações (POSIC) e normas complementares;*
>
> *5.1.3 As diretrizes relativas à sua Gestão de Riscos de Segurança de Informação e Comunicações (GRSIC);*
>
> *5.1.4 As informações tratadas em ambiente de computação em nuvem devem passar por um processo de GRSIC;*
>
> *5.1.5 As diretrizes relativas à sua Gestão de Continuidade, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC);*
>
> *5.1.6 As legislações vigentes para contratação de Solução de Tecnologia de Informação;*
>
> *5.1.7 As legislações vigentes relativas à Gestão da Segurança da Informação e Comunicações;*
>
> *5.1.8 As diretrizes para implementação de controles de acesso relativos à SIC; e*
>
> *5.1.9 A prevalência da legislação brasileira sobre qualquer outra.* (grifos nossos)

2.13. Por sua vez, o tratamento da informação em ambiente de computação em nuvem exige que a informação seja previamente classificada nos termos da Lei de Acesso à Informação (Lei nº.12.527, de 18 de novembro de 2011, regulamentada pelo Decreto nº.7.724, de 16 de maio de 2012) e demais normas aplicáveis, a exemplo de legislação específica que disciplina hipóteses envolvendo sigilo fiscal, bancário, comercial, empresarial e contábil. Feita tal classificação, cumpre ao responsável pelo tratamento da informação observar as seguintes diretrizes:

> *5.2.1 Informação sem restrição de acesso: pode ser tratada, a critério do órgão ou entidade da APF, em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC;*
>
> *5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:*
>
> *5.2.2.1 Informação classificada: é vedado o tratamento em ambiente de computação de nuvem;*
>
> *5.2.2.2 Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;*
>
> *5.2.2.3 Informação com restrição de acesso prevista em legislação vigente: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade (DICA);*
>
> *5.2.2.4 Documento preparatório: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem DICA;*
>
> *5.2.2.5 Documento preparatório que possa originar informação classificada deve ser tratado conforme o item 5.2.2.1; e*
>
> *5.2.2.6 Informação pessoal relativa à intimidade, vida privada, honra e imagem: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA. (grifos nossos)*

2.14. A Norma do GSI orienta, ainda, no item 5.2.3 que todos os dados,

metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da Administração Pública Federal, inclusive suas cópias de segurança, devem residir em território brasileiro. Quando se tratar de informação com restrição de acesso prevista em legislação vigente (item 5.2.2.3), documento preparatório (item 5.2.2.4) e informação pessoal relativa à intimidade, vida privada, honra e imagem (item 5.2.2.6), os dados devem residir exclusivamente em território brasileiro.

2.15. Destaca-se ainda o item 5.6 que veda o tratamento de informação em ambientes de computação em nuvem não autorizados pela Alta Administração do órgão ou entidade da Administração Pública Federal, a quem compete zelar pela segurança das informações tratadas em ambiente de nuvem (item 6.1).

2.16. A Controladoria-Geral da União adotou a ferramenta *Microsoft Teams* para realização de videoconferências em processos administrativos disciplinares, bem como as demais ferramentas do pacote da Microsoft Office para operacionalizar o trabalho remoto no órgão. Atualmente, os vídeos referentes às videoconferências são gravados na ferramenta OneDrive referente a cada usuário da organização, ferramenta cujos dados são armazenados em território brasileiro, conforme informações obtidas no sítio da Microsoft Office sobre a localização, por área geográfica, dos dados de clientes da Microsoft por tipo de serviço (Despacho 1423100 - https://docs.microsoft.com/pt-br/microsoft-365/enterprise/o365-data-locations?ms.officeurl=datamaps&rtc=1&view=o365-worldwide#brazil):

o

Serviço	Local
Exchange Online	Brasil
OneDrive for Business	Brasil
SharePoint Online	Brasil
Skype for Business	Estados Unidos
Microsoft Teams	Brasil
Office Online & Mobile	Brasil
EOP	Brasil
Intune	Estados Unidos
MyAnalytics	Brasil
Planner	Estados Unidos
Sway	Estados Unidos
Yammer	Estados Unidos
Serviços do OneNote	Brasil
Stream	Estados Unidos
Quadro de comunicações	Estados Unidos
Formulários	Estados Unidos
Workplace Analytics	Estados Unidos

2.17. Depreende-se do rol acima que somente uma parte das ferramentas oferecidas pela Microsoft armazena seus dados em território brasileiro. Nesse sentido, considerando que a condução de processos correcionais, englobando procedimentos disciplinares e procedimentos de responsabilização de entes privados, envolve potencialmente o tratamento de informação com restrição de acesso prevista em legislação vigente (item 5.2.2.3), documento preparatório

(item 5.2.2.4) e informação pessoal relativa à intimidade, vida privada, honra e imagem (item 5.2.2.6), recomenda-se a todas as unidades do SISCOR que, ao utilizar ambiente de computação em nuvem, observem a necessidade de tais dados serem armazenados exclusivamente em território nacional, em conformidade ao item 5.2.2 da Norma Complementar nº.14/IN01/DSIC/SCS/GSIPR, de 13 de março de 2018, além de observar os demais princípios, diretrizes e responsabilidades relacionados à Segurança da Informação estabelecidos pela norma.

2.18. Por fim, especificamente no tocante ao procedimento para classificação de informação, destaca-se a necessidade de observância da Orientação Conjunta nº 1//2021/ME/CGU, de 12 de março de 2021 (1954676), a qual aborda o tema Transparência no Processo Administrativo Eletrônico, e explicita como realizar a restrição de acesso dos documentos inseridos em processo eletrônico no Sistema Eletrônico de Informações - SEI, de acordo com a legislação aplicável.

3. DA CONCLUSÃO

3.1. Diante de todo o exposto, submete-se o presente entendimento à consideração superior, com sugestão de adoção das seguintes providências:

I - remessa de cópia da presente nota bem como dos documentos SEI 1953292 e 1954676 ao órgão consulente;

II - atualização do Manual de Processo Administrativo Disciplinar desta Controladoria-Geral da União para registrar os avanços na condução dos procedimentos correcionais em meio eletrônico e a correspondente necessidade de zelar pela disponibilidade, integridade, confidencialidade e autenticidade no tratamento da informação em ambiente de computação em nuvem, conforme legislação referenciada na presente Nota.

Documento assinado eletronicamente por **STEFANIE GROENWOLD CAMPOS**, **Auditor Federal de Finanças e Controle**, em 24/05/2021, às 19:47, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 1942008 e o código CRC 9F7B5E45

Referência: Processo nº 00190.112020/2019-51 SEI nº 1942008

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Secretaria de Coordenação de Sistemas
Departamento de Segurança da Informação e Comunicações

PRINCÍPIOS, DIRETRIZES E RESPONSABILIDADES RELACIONADOS À SEGURANÇA DA INFORMAÇÃO PARA O TRATAMENTO DA INFORMAÇÃO EM AMBIENTE DE COMPUTAÇÃO EM NUVEM.

ORIGEM

Departamento de Segurança da Informação e Comunicações.

REFERÊNCIA LEGAL, NORMATIVA E BIBLIOGRÁFICA

Lei nº 12.527, de 18 de novembro de 2011.
Lei nº 12.965, de 23 de abril de 2014.
Decreto nº 3.505, de 13 de junho de 2000.
Decreto nº 7.724, de 16 de maio de 2012.
Decreto nº 7.845, de 14 de novembro de 2012.
Decreto nº 8.135, de 4 de novembro de 2013.
Decreto nº 9.203, de 22 de novembro de 2017.
Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República nº 01, de 13 de junho de 2008 e respectivas Normas Complementares.
Instrução Normativa nº 04 do Ministério do Planejamento Desenvolvimento e Gestão, de 11 de setembro de 2014.
CONSELHO NACIONAL DE ARQUIVO (Brasil). Glossário: Documentos Arquivísticos Digitais, 6ª versão, Rio de Janeiro: CONARQ, 2014.

CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC14/IN01/DSIC/SCS/GSIPR, de 30 de janeiro de 2012.

APROVAÇÃO

14 MAR 2018

NORIAKI WADA
Secretário de Coordenação de Sistemas

1 OBJETIVO

Estabelecer princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

2 CONSIDERAÇÕES INICIAIS

As tecnologias de computação em nuvem oferecem benefícios, como economicidade e eficiência, que podem ser aproveitados pelos órgãos ou entidades da APF. Associado a tais vantagens, o uso dessas novas tecnologias pode ocasionar o surgimento de riscos. Portanto, a Alta Administração de cada órgão ou entidade da APF deve considerar a Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC), de modo a salvaguardar dados, informações e serviços sob sua responsabilidade, visando a continuidade do negócio e preservando a Segurança da Informação e os interesses da sociedade e do Estado.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Incisos I e II do parágrafo único do art. 87 da Constituição Federal, no inciso IV do art. 10 da Lei nº 13.502, de 1 de novembro de 2017 e no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional da Presidência da República.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

4.1 **Alta Administração**: Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo-Direção e Assessoramento Superiores - DAS e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente;

4.2 **Autenticidade**: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

4.3 **Computação em Nuvem**: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

4.4 **Confidencialidade**: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizado nem credenciado;

4.5 **Continuidade de Negócios**: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

4.6 **Controle de Acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos meios de tecnologia oferecidos;

4.7 **Disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

4.8 **Gestão de Continuidade**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

4.9 **Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)**: conjunto de processos que permitem identificar, analisar, avaliar e implementar as medidas necessárias para o tratamento de riscos e equilibrá-los com os custos operacionais e financeiros envolvidos;

4.10 **Gestão de Segurança da Informação e Comunicações**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, classificação e tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança de recursos humanos e segurança documental aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações;

4.11 **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

4.12 **Informação Classificada**: é a informação sigilosa, à qual foi atribuída um grau de sigilo, conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

4.13 **Informação Sigilosa**: informação submetida à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

4.14 **Integridade**: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

4.15 **Metadado**: Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

4.16 **Política de Segurança da Informação e Comunicações (POSIC)**: documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de estabelecer ações que visam a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações

produzidas ou custodiadas por estes, independentemente da forma e do meio físico em que estejam registradas;

4.17 **Provedor**: ente, público ou privado, prestador de serviço de computação em nuvem;

4.18 **Risco**: probabilidade da ocorrência de um evento que tenha impacto na segurança da informação;

4.19 **Segurança da Informação e Comunicações**: consiste em assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação;

4.20 **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; e

4.21 **Tratamento de Incidentes de Segurança em Redes Computacionais**: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

5 PRINCÍPIOS E DIRETRIZES

5.1 O órgão ou entidade da APF deve observar, no mínimo, ao adotar o tratamento da informação em ambiente de Computação em Nuvem:

5.1.1 A prevalência dos direitos e garantias fundamentais no tratamento das informações pessoais;

5.1.2 As diretrizes estabelecidas em sua Política de Segurança da Informação e Comunicações (POSIC) e normas complementares;

5.1.3 As diretrizes relativas à sua Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC);

5.1.4 As informações tratadas em ambiente de computação em nuvem devem passar por um processo de GRSIC;

5.1.5 As diretrizes relativas à sua Gestão de Continuidade, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC);

5.1.6 As legislações vigentes para contratação de Solução de Tecnologia da Informação;

5.1.7 As legislações vigentes relativas à Gestão de Segurança da Informação e Comunicações;

5.1.8 As diretrizes para implementação de controles de acesso relativos à SIC; e

5.1.9 A prevalência da legislação brasileira sobre qualquer outra.

5.2 Sobre o tratamento da informação:

5.2.1 Informação sem restrição de acesso: pode ser tratada, a critério do órgão ou entidade da APF, em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC;

5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:

5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem;

5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;

5.2.2.3. Informação com restrição de acesso prevista em legislação vigente: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade (DICA);

5.2.2.4. Documento Preparatório: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA;

5.2.2.5. Documento preparatório que possa originar informação classificada deve ser tratado conforme o item 5.2.2.1; e

5.2.2.6. Informação pessoal relativa à intimidade, vida privada, honra e imagem: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA.

5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro;

5.4 Os dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, referentes aos itens 5.2.2.3, 5.2.2.4 e 5.2.2.6, devem residir exclusivamente em território brasileiro;

5.5 Na adoção de serviços de computação em nuvem, o órgão ou entidade da APF deve assegurar que sejam definidos, em instrumento contratual ou similar:

5.5.1 Requisitos que garantam a DICA das informações tratadas em ambiente de computação em nuvem;

5.5.2 Processo de comunicação e tratamento de incidentes de segurança em redes computacionais, considerando as exigências da legislação vigente;

5.5.3 Requisitos necessários para a realização de auditorias;

5.5.4 Que os dados, metadados, informações e conhecimento, tratados pelo provedor, não poderão ser fornecidos a terceiros e/ou usados por este provedor para fins diversos do previsto no referido instrumento contratual ou similar, sob nenhuma hipótese, sem autorização formal do órgão ou entidade da APF;

5.5.5 Requisitos necessários para a continuidade de negócio;

5.5.6 Requisitos necessários, para os casos de cancelamento, descontinuidade, portabilidade e renovação do referido instrumento contratual ou similar, bem como substituição de ambiente, que visem à eliminação e/ou à destruição definitiva dos dados, metadados, informações e conhecimento; e

5.6 É vedado o tratamento de informação em ambientes de computação em nuvem não autorizados pela Alta Administração do respectivo órgão ou entidade da APF.

6 RESPONSABILIDADES

6.1 A Alta Administração de cada órgão ou entidade da APF, no âmbito de suas competências, é responsável pela segurança das informações tratadas em ambiente de computação em nuvem, em conformidade com as orientações contidas nesta norma e legislação vigente; e

6.2 O Gestor de Segurança da Informação e Comunicação do órgão, no âmbito de suas atribuições, é responsável pelas ações de implementação da gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

Orientação Conjunta nº 1//2021/ME/CGU

TRANSPARÊNCIA NO PROCESSO ADMINISTRATIVO ELETRÔNICO

1 LEGISLAÇÃO APLICÁVEL

A Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI) – indica, em seu art. 3º, que a publicidade é o preceito geral e o sigilo a exceção. Além disso, define como diretriz que as informações de interesse público devem ser divulgadas, independentemente de solicitações:

> Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
>
> I - **observância da publicidade como preceito geral e do sigilo como exceção**;
> II - **divulgação de informações de interesse público, independentemente de solicitações**;
> III - **utilização de meios de comunicação viabilizados pela tecnologia da informação**;
> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
> V - desenvolvimento do controle social da administração pública.

O Decreto nº 7.724, de 16/05/2012, que regulamenta a Lei de Acesso à Informação, estabelece no art. 7º, inciso I:

> Art. 7º É dever dos órgãos e entidades **promover, independente de requerimento, a divulgação** em seus sítios na Internet **de informações de interesse coletivo ou geral** por eles produzidas ou custodiadas, observado o disposto nos arts. 7º e 8º da Lei nº 12.527, de 2011.
>
> § 1º Os órgãos e entidades deverão implementar em seus sítios na Internet seção específica para a divulgação das informações de que trata o **caput."**

Ainda, a mesma LAI, em seu art. 31, dispõe que:

> **Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.**
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
> (...)
> § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal. **(Grifou-se)**

A Lei nº 13.709, de 14 de agosto de 2018 - Lei-Geral de Proteção de Dados Pessoais - que regula as atividades de tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, possui diversos dispositivos que devem ser observados pelos sistemas de processo administrativo. Vejamos os principais:

> **Conceitos LGPD**
>
> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> 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;
> (...)
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de

tratamento;
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
IX - agentes de tratamento: o controlador e o operador;
X - tratamento: toda 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, transferência, difusão ou extração;
XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
(...)

Princípios do tratamento de dados pessoais

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

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.

Tratamento de dados pessoais e processo administrativo

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
(...)
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)

2 NÍVEIS DE ACESSO

A tabela abaixo exemplifica as principais utilizações práticas dos níveis de acesso, que podem ser utilizadas por todos os sistemas de processo administrativo eletrônico, de acordo com suas configurações próprias:

Nível de	Tipo de informação	Fundamentação	Quem pode acessar	Exemplos de

Acesso	Tipo de informação	Legal	Quem pode acessar	documentos
Público	De interesse público, geral ou coletivo	art. 8º, §1º, inciso IV, da Lei 12.527/2011 c/c art. 7º, §3º, inciso V do Decreto 7.724/2012	Todas as pessoas	- informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados; - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades
Restrito	Informações pessoais, relacionadas a uma determinada pessoa identificada ou identificável;	Art. 31 da Lei nº 12.527, de 2011	• agentes públicos legalmente autorizados • própria pessoa a quem a informação se referir, mediante identificação	documentos que contenham informações pessoais de pessoa identificada ou identificável, como: • RG, • CPF, • estado de saúde do servidor ou familiares, • informações financeiras • informações patrimoniais • alimentandos, • dependentes • pensões • endereços • número de telefone • e-mail • origem racial ou étnica, orientação sexual • convicções religiosas, filosóficas ou morais, opiniões políticas • filiação sindical • filiação partidária • filiação a organizações de caráter religioso, filosófico ou político.
	Documento Preparatório utilizado	Art. 20 do	• agentes públicos legalmente autorizados	• notas técnicas, pareceres, notas informativas ou outros documentos que subsidiem decisões dos dirigentes em documentos sobre políticas

Restrito	Preparatório utilizado como fundamento de tomada de decisão ou de ato administrativo	Art. 20 do Decreto 7724/2012	• interessado, mediante identificação	econômica, fiscal, tributária, monetária, regulatória etc. • documentos que tragam argumentos e conteúdo para os processos que culminarão na edição de ato normativo;
Restrito	Informações protegidas por legislação específica como sigilo fiscal, bancário, comercial, empresarial e contábil.	Diversas	• agentes públicos legalmente autorizados • interessado, mediante identificação	• ofícios, extratos, relatórios, atas etc que contenham informações fiscais, bancárias, comerciais, empresariais ou contábeis protegidas por sigilo.

3 ORIENTAÇÕES GERAIS NÍVEIS DE ACESSO NO PROCESSO ADMINISTRATIVO ELETRÔNICO

As legislações e orientações acima devem ser observadas por qualquer sistema de processo eletrônico adotado.

Adicionalmente, considerando que, atualmente, 118 dos 192 órgãos e entidades que integram a Administração Pública federal direta, autárquica e fundacional utilizam o Sistema Eletrônico de Informações-SEI, desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4), dos quais 111 já têm o sistema implantado e outros 7 encontram-se em processo de implantação, passa-se, a seguir, nos itens 4 a 6, a tecer orientações específicas quanto a esse sistema.

4 NÍVEIS DE ACESSO NO SISTEMA ELETRÔNICO DE INFORMAÇÕES-SEI

Todos os processos e documentos no SEI devem, obrigatoriamente, ter o nível de acesso informado, de acordo com as opções **sigiloso, restrito e público.**

O nível de acesso **"Público"** permite que os processos e documentos assim categorizados fiquem disponíveis, em inteiro teor, para todos os usuários internos habilitados no SEI e por qualquer usuário externo que realize pesquisa no Módulo de Consulta Pública do SEI, para os órgãos e entidades que possuem o módulo instalado.

Processos e documentos categorizados com o nível de acesso **"Restrito"** têm seu conteúdo visível somente aos usuários internos das unidades pelas quais o processo tramitou ou a usuários externos credenciados. As informações restritas no SEI que tratem de direitos ou obrigações individuais, devem ser concedidas somente aos interessados devidamente identificados.

Processos e documentos categorizados como "**Sigiloso**" são indicados por meio do símbolo de chave vermelha ao lado direito de seus respectivos números na árvore do SEI. Essa categoria de restrição permite que a visualização dos processos ocorra apenas pelos usuários credenciados. No entanto, é importante esclarecer que o nível de acesso **Sigiloso** não corresponde aos graus de sigilo reservado, secreto e ultrassecreto de que tratam os Art. 23 e 24 da Lei de Acesso à Informação e que documentos que contenham informações em grau de sigilo não devem ser inseridos no SEI, tendo em vista não haver recomendação do Gabinete de Segurança Institucional da Presidência da República (GSI).

Para saber mais sobre o tratamento de informação classificada em grau de sigilo, acesse a página do GSI no endereço https://www.gov.br/gsi/pt-br/assuntos/dsi

A permissão sobre quais níveis de acesso podem ser aplicáveis a cada tipo de documento e tipo de processo no SEI é definida em parametrização realizada pelo Administrador do Sistema em cada instituição. Essa parametrização deve ser realizada em estrita observância à Lei de Acesso à Informação, à Lei Geral de Proteção de Dados e às demais legislações que tratam de hipóteses de sigilo.

Cabe lembrar que o Administrador do Sistema pode definir padrões pré-selecionados para os diferentes tipos de processo. Assim, os processos de pedido de afastamento médico, por exemplo, podem já vir com acesso restrito como opção padrão – e é possível até mesmo excluir a possibilidade de, para um determinado tipo de processo, que ele seja público ou que ele seja restrito.

É importante também que a habilitação dos tipos de documentos para as unidades no SEI guarde relação com suas atribuições legais, visando evitar o uso de nomenclatura indevida do tipo de documento. Por esse motivo, nomenclaturas amplas como “anexo”, “documentos”, “formulário” devem ser objeto de acurado procedimento de habilitação e se, possível, retiradas.

A atribuição do nível de acesso durante a criação do processo ou documento do SEI é realizada pelo usuário que está gerando a informação. Os usuários devem ser orientados a gerar os documentos associados aos tipos documentais específicos.

É imperativo que os órgãos capacitem seus servidores para o uso adequado do sistema, em especial aqueles que utilizam o módulo de consulta pública do SEI, a fim de equilibrar as obrigações legais de transparência e preservação de dados restritos. Tais capacitações devem levar em conta o arcabouço legal, as características do sistema e a forma como ele foi configurado para funcionamento no órgão.

5 CONFIGURAÇÕES DO MÓDULO DE CONSULTA PÚBLICA DO SEI

O Módulo de Consulta Pública, integrado ao Sistema Eletrônico de Informações-SEI, é uma solução desenvolvida pelo Conselho Administrativo de Defesa Econômica (CADE) e disponibilizada gratuitamente para os demais órgãos e entidades que assim desejarem no âmbito da atuação colaborativa e integrada da Comunidade do Processo Eletrônico Nacional. Ele permite que pessoas externas ao órgão consultem e acompanhem processos e informações públicas contidas no SEI a que vier a ser acoplado.

Muito embora o SEI contenha nativamente funcionalidades que indicam o nível de acesso a determinado processo ou documento, ele não possui recurso que permita a consulta pela internet do inteiro teor de informações públicas. Assim, o Módulo de Consulta Pública, nos órgãos que o implementaram, permite a pesquisa de informações existentes no Sistema por meio da aposição de pelo menos um parâmetro de pesquisa dentre os disponíveis, como: número do processo, tipo de processo, unidade geradora, texto livre etc.

Os resultados de conteúdo e andamentos (trâmites) apresentados pelo Módulo de Consulta Pública do SEI dependem da categorização de nível de acesso público, restrito ou sigiloso realizado pelo usuário interno do SEI e estão detalhados abaixo.

Processo	Documento	Conteúdo	Andamentos
Público	Público	Disponível	Disponível
Público	Restrito	Não disponível	Disponível
Restrito	Público ou Restrito	Não disponível	Disponível
Sigiloso	Público, Restrito ou Sigiloso	Não apresenta resultados	Não apresenta resultados

Portanto, o módulo disponibiliza o inteiro teor dos documentos categorizados como públicos no SEI, desde que estejam inseridos em processos também públicos. Documentos restritos contidos em processos públicos ou processos restritos não apresentam o conteúdo, mas somente os seus respectivos andamentos (trâmites). Tais regras resultam essencialmente das características funcionais do SEI. Dessa forma, a correta categorização dos documentos e processos no SEI é condição essencial para seja dada publicidade às informações públicas, resguardando, por outro lado, informações restritas, sigilosas ou de caráter pessoal.

Alternativamente, o módulo em sua versão atual, permite implementar configuração que retorne na pesquisa apenas a lista de andamentos (trâmites) dos documentos públicos contidos em processos públicos, e não o inteiro teor dos mesmos.

O bom funcionamento do módulo, porém, é intrinsicamente ligado à preparação da equipe que opera o sistema. Levantamento da CGU revelou a abertura de informações pessoais sensíveis na maior parte dos órgãos que utilizam o módulo.

6 TRATAMENTO DADO NO BARRAMENTO DE SERVIÇOS DO PEN AOS PROCESSOS COM NÍVEL DE ACESSO “RESTRITO” NO SEI

O Barramento de Serviços do Processo Eletrônico Nacional (PEN) é uma solução tecnológica desenvolvida pelo Ministério da Economia que permite a tramitação de documentos e processos entre diferentes sistemas de processo eletrônico como SEI, SAPIENS, eDOC, SIPAC, SUAP etc.

A indicação do nível de acesso da informação é campo obrigatório para o trâmite no Barramento. Por isso, temos atualmente na base comum a seguinte relação de hipóteses legais de restrição de acesso, que correspondem ao nível de acesso "Restrito" do SEI.

Nome	Base legal
Processo Administrativo de Responsabilização (PAR)	Art. 4º, §1º, do Decreto nº 8.420/2015

Tratados, acordos e atos internacionais	Art. 36, Lei 12527/2011
Investigação/Prevenção de Acidentes Aeronáuticos	Art. 88-I, § 3º, da Lei nº 7.565/1986
Investigação Preliminar sobre Mercado Mobiliário	Art. 9º, § 2º, da Lei 6.385/1976
Atividade Empresarial	Art. 5º, § 2º, do Decreto nº 7.724/2012
Situação Econômico-Financeira de Sujeito Passivo	Art. 198, caput, da Lei nº 5.172/1966 - CTN
Sigilo do Inquérito Policial	Art. 20 do Código de Processo Penal
Sigilo de Empresa em Situação Falimentar	Art. 169 da Lei nº 11.101/2005
Sigilo das Comunicações	Art. 3º, V, da Lei nº 9.472/1997
Segredo Industrial	Art. 195, XIV, Lei nº 9.279/1996
Segredo de Justiça no Processo Penal	Art. 201, § 6º, do Código de Processo Penal
Segredo de Justiça no Processo Civil	Art. 189 do Código de Processo Civil
Protocolo-Pendente Análise de Restrição de Acesso	Art. 6º, III, da Lei nº 12.527/2011
Investigação de Responsabilidade do Servidor	Art. 150 da Lei nº 8.112/1990
Interceptações de Comunicações Telefônicas	Art. 8º, caput, da Lei nº 9.296/1996
Informação Privilegiadas de Sociedades Anônimas	Art. 155, § 2º, da Lei nº 6.404/1976
Informação Pessoal	Art. 31 da Lei nº 12.527/2011
Documento Preparatório	Art. 7º, § 3º, da Lei nº 12.527/2011
Direito Autoral	Art. 24, III, da Lei nº 9.610/1998
Controle Interno	Art. 26, § 3º, da Lei nº 10.180/2001
Livros e Registros Contábeis Empresariais	Art. 1.190 do Código Civil
Operações Bancárias	Art. 1º da Lei Complementar nº 105/2001
Proteção da Propriedade Intelectual de Software	Art. 2º da Lei nº 9.609/1998

Caso o órgão adote o Barramento de Serviços do PEN e não localize hipótese legal utilizada em seu sistema, deve solicitar a inclusão por meio da Central de Atendimento, endereço https://portaldeservicos.economia.gov.br/.

Documento assinado eletronicamente por **Cristiano Rocha Heckert**, **Secretário(a)**, em 11/03/2021, às 18:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **CLAUDIA TAYA**, **Usuário Externo**, em 12/03/2021, às 11:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **14235569** e o código CRC **471D0A76**.

Referência: Processo nº 19973.102307/2021-16. SEI nº 14235569

CONTROLADORIA-GERAL DA UNIÃO

DESPACHO CGUNE

1. Estou de acordo com a Nota Técnica nº 1.176/2021/CGUNE/CRG, que responde à consulta formulada por unidade seccional de correição, no sentido de ser possível a utilização de ferramentas tecnológicas, incluindo as ferramentas do Escritório Digital da Microsoft, para a realização e gravação de depoimentos em processos correcionais, observando-se as normas existentes sobre o tratamento de dados pessoais.

2. À apreciação do Senhor Corregedor-Geral da União.

Documento assinado eletronicamente por **CARLA RODRIGUES COTTA**, **Coordenador-Geral de Uniformização de Entendimentos**, em 24/05/2021, às 18:42, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 1961651 e o código CRC 4250B957

Referência: Processo nº 00190.112020/2019-51 SEI nº 1961651

CONTROLADORIA-GERAL DA UNIÃO

DESPACHO CRG

1. Aprovo a Nota Técnica nº 1.176/2021/CGUNE/CRG 1942008.

2. **À COPIS** para dar ciência do entendimento desta CRG à Corregedoria do Ministério da Economia.

Documento assinado eletronicamente por **GILBERTO WALLER JUNIOR**, **Corregedor-Geral da União**, em 28/05/2021, às 14:39, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 1961678 e o código CRC D6807E44

Referência: Processo nº 00190.112020/2019-51 SEI nº 1961678