CONTROLADORIA-GERAL DA UNIÃO
NOTA TÉCNICA Nº 956/2022/CGUNE/CRG

PROCESSO Nº 00190.102641/2022-21

INTERESSADO: Corregedoria do Ministério da Saúde.

1. **ASSUNTO**

1.1. Uso de ferramentas tecnológicas para condução de processos correcionais.

2. **REFERÊNCIAS**

2.1. Lei nº.12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI);

2.2. Lei nº.13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD);

2.3. Norma Complementar n. 14/IN01/DSIC/SCS/GSIPR, de 13 de março de 2018;

2.4. Instrução Normativa nº 5, de 30 de agosto de 2021, DOU de 31/08/2021, Seção 1, p.2;

2.5. Nota Técnica nº 1176/2021/CGUNE/CRG, de 24 de maio de 2021 (SEI 1942008).

3. **ANÁLISE**

3.1. Trata-se de consulta formulada pela Corregedoria-Geral do Ministério da Saúde por meio do Ofício nº 217/2022/CORREG/DINTEG/MS, de 23 de março de 2022, com o seguinte teor:

> *"1. Ao tempo que o cumprimento respeitosamente, sirvo-me do presente expediente para solicitar a Vossa Senhoria esclarecimentos a respeito da* ***Nota Técnica nº 1176/2021/CGUNE/CRG.***
>
> *2. A presente consulta circunscreve-se aos itens 2.14 a 2.18 que salientam 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, e que 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, e que, 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.*
>
> *3. Ante o acima declinado, solicita-se o esclarecimento do ponto em questão, no que concerne à possibilidade de utilização de outras plataformas ou aplicativos, além do Teams, a exemplo do Skype e do Google Meet, para realização de Videoconferências com acusados ou indiciados, ou mesmo para outros trabalhos correcionais que careçam de registro e arquivo, tais como aplicativos, visto que os dados provenientes dessas ferramentas são armazenados nos Estados Unidos."*

3.2. Cinge-se à consulta à correta interpretação dos itens 2.14 a 2.18 da Nota Técnica nº 1176/2021/CGUNE/CRG, de 24 de maio de 2021, especificamente para indagar acerca da possibilidade de utilização de outras ferramentas tecnológicas para realização de videoconferências, a exemplo do Skype e do Google Meet, cujos dados são armazenados nos Estados Unidos. Para maior clareza, transcrevem-se os supracitados itens da Nota Técnica:

> *"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):

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."

3.3. Por se tratar de dúvida afeta à natureza de ferramentas tecnológicas, esta Coordenação-Geral de Uniformização de Entendimentos solicitou orientação sobre o tema por parte da Diretoria de Tecnologia da Informação desta CGU, tendo encaminhado mensagem eletrônica (SEI 2362508) indagando especificamente se a utilização das referidas ferramentas estaria em conformidade com os ditames da Norma Complementar nº. 14/IN01/DSIC/SCS/GSIPR, de 13 de março de 2018.

3.4. Em resposta, a DTI apontou a existência de norma posterior à referida Norma Complementar - a Instrução Normativa nº. 05, de 30 de agosto de 2021, editada pelo Gabinete de Segurança Institucional da Presidência da República em data posterior à manifestação exarada pela Nota Técnica nº.1.176/2021/CGUNE/CRG, e destacou que a ferramenta Skype for Business será descontinuada pela fabricante Microsoft. Transcreve-se a seguir o teor da mensagem SEI 2362508:

> *"Analisando a NOTA TÉCNICA Nº 1176/2021/CGUNE/CRG que foi elaborada em 28/05/2021 vimos que usaram como base a NC 14 porque ainda não tinham publicado a INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal, link .*
>
> *Veja que em seu art 8º, ele atribui ao Comitê de segurança do órgão a tarefa de definir os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados*
>
> *Art. 8º Ao Comitê de Segurança da Informação ou à estrutura equivalente compete:*
>
> *I - estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem;*
>
> *II - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem; e*
>
> *III - analisar, em caráter conclusivo, as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.*
>
> *Outra informação importante é que o Skype for Business vai ser descontinuado pela Microsoft.*
>
> *Conforme artigo da Microsoft escrito em 25/03/2022. Link*
>
> *"Em 31 de julho de 2021, a Microsoft reformou Skype for Business Online. Essa aposentadoria foi anunciada em julho de 2019 para dar aos clientes dois anos de antecedência aviso para planejar suas atualizações para Microsoft Teams. Teams é o aplicativo principal para comunicação e colaboração no Microsoft 365. Com Skype for Business Online sendo retirada, a Microsoft deseja garantir que os clientes tenham as informações e recursos necessários para planejar e executar uma atualização bem-sucedida para Teams. O Skype de consumidor não é afetado por essa aposentadoria. Para saber mais sobre por Skype for Business Online foi Skype for Business, consulte Perguntas frequentes— Atualizando de Skype for Business para Microsoft Teams.*
>
> *A Microsoft começará a descomissionar a infraestrutura Skype for Business Online em ou após 30 de junho de 2022. Este artigo contém orientações para organizações com usuários do TeamsOnly que foram atualizados de qualquer versão do Skype for Business."*

3.5. A Instrução Normativa nº.05, de 30 de agosto de 2021, dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da Administração Pública Federal. Transcrevem-se abaixo os dispositivos mais relevantes da norma:

> *"Art. 4º Todos os órgãos ou as entidades, que desejarem utilizar computação em nuvem,* ***deverão editar, obrigatoriamente, um ato normativo sobre o uso seguro de computação em nuvem.***
>
> *(...)*
>
> *Art. 6º O órgão ou a entidade deverá* ***instituir uma equipe para elaboração e revisões do ato normativo*** *sobre o uso seguro de computação em nuvem.*
>
> *Art. 7º Ao Gestor de Segurança da Informação compete:*
>
> *I -* ***instituir e coordenar a equipe descrita no art. 6º,*** *responsável pela elaboração e revisões do ato normativo sobre uso seguro de computação em nuvem;*
>
> *II - supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem;*
>
> *III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao órgão ou à entidade, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;*

IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;

V - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida; e

*VI - **encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.***

*Art. 8º Ao **Comitê de Segurança da Informação ou à estrutura equivalente compete:***

*I - **estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem;***

II - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem; e

III - analisar, em caráter conclusivo, as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

(...)

*Art. 11. **Antes de transferir serviços ou informações para um provedor de serviço de nuvem, os órgãos ou as entidades deverão, no mínimo:***

I - garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros as seguintes operações:

a) de coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e

b) de comunicações realizada por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional;

*II - realizar o gerenciamento de riscos**,** precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação, dos seguintes itens:*

a) o tipo de informação a ser migrada;

b) o fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;

c) o valor dos ativos envolvidos; e

d) os benefícios da adoção de uma solução de computação em nuvem, em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro;

III - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - utilizar, para os sistemas estruturantes, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas de órgãos ou de entidades;

V - avaliar quais informações serão hospedadas na nuvem, considerando:

a) o processo de classificação da informação de acordo com a legislação;

b) o valor do ativo de informação;

c) os controles de acessos físico e lógico relativos à segurança da informação; e

d) o modelo de serviço e de implementação de computação em nuvem;

VI - definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução; e

VII - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

(...)

Art. 17. Em relação ao tratamento da informação em ambiente de computação em nuvem, o órgão ou a entidade, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:

*I - i**nformação sem restrição de acesso poderá ser tratada em ambiente de nuvem**, considerada a legislação e os riscos de segurança da informação;*

*II - **informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem;** e*

*III - **poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:***

> ***a) a informação com restrição de acesso prevista na legislação, conforme o Anexo a esta Instrução Normativa****;*
>
> *b) o material de acesso restrito regulado pelo próprio órgão ou pela entidade;*
>
> *c) a informação pessoal relativa à intimidade, vida privada, honra e imagem; e*
>
> *d) o documento preparatório não previsto no inciso II do* ***caput****.*
>
> *Art. 18.* ***Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro,*** *observando-se as seguintes disposições:*
>
> *I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;*
>
> *II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;*
>
> *III -* ***a informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II do caput art. 17, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável****; e*
>
> *IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.*
>
> *(grifos nossos)*"

3.6. Depreende-se do texto normativo que os órgãos e entidades do Poder Executivo Federal podem utilizar a computação em nuvem, desde que editem ato normativo específico sobre o uso seguro da ferramenta (art. 4º). Compete ao Gestor de Segurança da Informação de cada órgão ou entidade instituir e coordenar a equipe responsável pela edição e revisão do referido ato, que será aprovado pela alta administração do órgão/entidade (art. 7º, incisos I e VI). Por sua vez, compete ao Comitê de Segurança da Informação estabelecer em quais países poderão ser armazenados os dados e informações custodiados por aquele órgão/entidade (art.8º, inciso I).

3.7. O artigo 11 alerta que, previamente à qualquer transferência de serviços ou informações para um provedor de acesso à nuvem, o órgão ou entidade deverá se certificar de que as operações de coleta, armazenamento, guarda e tratamento de dados pessoais, bem como as operações de comunicações estejam em conformidade com a legislação brasileira de proteção de dados e direitos à privacidade e sigilo (art.11, inciso I). Também deverá ser realizada a classificação - de acordo com os critérios legais - daquela informação que será hospedada na nuvem (art.11, inciso V), além de outras providências exigidas pelo art.11 que buscam assegurar o uso seguro da ferramenta.

3.8. Especificamente sobre o tratamento da informação em ambiente de computação de nuvem, o artigo 17 diferencia três tipos de informação:

> a) **a informação sem restrição de acesso, que poderá ser tratada em ambiente de nuvem, podendo ser armazenada no Brasil ou no exterior**, conforme definido pelo Comitê de Segurança de Informação do órgão ou entidade, entendimento que decorre da aplicação conjunta do art.17, inciso I c.c. art. 8º, inciso I da Instrução Normativa;
>
> b) **a informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratadas em ambiente de nuvem;** nos termos do Anexo à Instrução Normativa, trata-se daquela informação classificada como reservada, secreta ou ultrassecreta, nos moldes do artigo 24, §1º da Lei nº.12.527/2011 (Lei de Acesso à Informação);
>
> c) **a informação com restrição de acesso prevista em legislação, o material de acesso restrito regulado pelo próprio órgão ou entidade, a informação pessoal relativa à intimidade, vida privada, honra e imagem e documento preparatório do qual não possa originar informação classificada podem ser tratados em ambiente de nuvem,** conforme artigo 17, inciso III.

3.9. Dentro da categoria de informação que pode ser tratada em ambiente de nuvem, o artigo 18, inciso III ressalva que a informação com restrição de acesso prevista em lei e documento preparatório do qual não possa originar informação classificada não podem ser tratados fora do território brasileiro.

Destaca-se que, nos termos do artigo 5º, inciso IX, da Lei nº.13.709/2018 (LGPD), tratamento de dados consiste em *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.* Em outras palavras, a norma veda qualquer operação no exterior que envolva dados relacionados à informação com restrição de acesso prevista em lei.

3.10. Por sua vez, extrai-se do Anexo à Instrução Normativa que constituem informações com restrição de acesso prevista em lei os sigilos decorrentes de direitos de personalidade (fiscal, bancário, comercial, empresarial e contábil); os sigilos de processos e procedimentos, que incluem o sigilo do processo administrativo disciplinar em curso, o sigilo do inquérito policial, e o segredo de justiça no processo civil e no processo penal; e informação de natureza patrimonial (segredo industrial, direito autoral, propriedade intelectual de programa de computador e propriedade intelectual). Ainda, a norma destaca explicitamente que se trata de rol não exaustivo, admitindo-se, portanto, a existência de outras hipóteses legais de restrição de acesso.

3.11. Em suma, a informação relacionada a processo administrativo disciplinar em curso é classificada como informação com restrição de acesso prevista em lei e, como tal, pode ser tratada em ambiente de nuvem somente em território brasileiro. Nesse sentido, reproduz-se o teor da diretriz 5.4 da Norma Complementar nº. 14/IN01/DSIC/SCS/GSIPR, segundo a qual a informação com restrição de acesso prevista em legislação vigente deve residir exclusivamente em território brasileiro.

3.12. Conclui-se, portanto, que as orientações constantes dos itens 2.14 a 2.18 da Nota Técnica nº 1176/2021/CGUNE/CRG permanecem válidas face o teor da Instrução Normativa nº.05, de 30 de agosto de 2021, não sendo possível tratar dados ou informações com restrição de acesso prevista em lei em ambiente de nuvem sediado no exterior. Assim, recomenda-se ao Consulente a verificação da adequação das ferramentas e procedimentos adotados diante da legislação supramencionada, em conjunto com as autoridades responsáveis pela segurança da informação naquele órgão.

4. CONCLUSÃO

4.1. Diante do exposto, submete-se o presente entendimento à consideração da Sra. Coordenadora-Geral de Uniformização de Entendimentos, com sugestão de i) remessa de cópia da presente Nota ao órgão consulente; e ii) inserção da referida Nota na Base de Conhecimento, para divulgação ao Sistema de Correição do Poder Executivo Federal, acerca da atualização das normas do Gabinete de Segurança Institucional quanto aos requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da Administração Pública Federal.

Documento assinado eletronicamente por **STEFANIE GROENWOLD CAMPOS**, **Auditor Federal de Finanças e Controle**, em 09/05/2022, às 17:31, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 2357476 e o código CRC 90AFE5F6

Referência: Processo nº 00190.102641/2022-21 SEI nº 2357476