CONTROLADORIA-GERAL DA UNIÃO

NOTA TÉCNICA Nº 29/2026/CGUNE/DICOR/CRG

PROCESSO Nº 00190.110340/2025-14

INTERESSADO: INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA

1. ASSUNTO

1.1. Acesso de colaboradores terceirizados a processos correcionais sigilosos.

2. REFERÊNCIAS

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

2.2. Lei nº 8.112, de 11 de dezembro de 1990.

2.3. Decreto nº 7.845, de 14 de novembro de 2012.

2.4. Portaria Normativa CGU nº 27, de 28 de dezembro de 2022.

2.5. Nota Técnica nº 1523/2021/CGUNE/CRG.

3. SUMÁRIO EXECUTIVO

3.1. Trata-se de consulta formulada pela Corregedoria-Geral do Instituto Nacional de Colonização e Reforma Agrária – INCRA, por meio do Ofício nº 76243/2025/CGE-GAB/CGE/SEDE/INCRA-INCRA (3821817), que solicita esclarecimento quanto à possibilidade de colaboradores terceirizados terem acesso a processos administrativos classificados como sigilosos (Juízo de Admissibilidade e Investigação Preliminar Sumária), especialmente aqueles protegidos por grau de sigilo "reservado", "secreto" ou "ultrassecreto", conforme previsto na Lei nº 12.527/2011.

3.2. O órgão consulente informa que os colaboradores terceirizados que prestam serviços na CGE-INCRA desempenham funções administrativas, incluindo a inserção de modelos previamente desenvolvidos de despachos em procedimentos de Juízo de Admissibilidade e em Investigação Preliminar Sumária. Ressalta que os colaboradores não assinam documentos, cabendo a checagem e validação final aos servidores efetivos.

3.3. Especificamente, o INCRA questiona: (i) se há previsão normativa que autorize, mediante termo de confidencialidade ou outro instrumento formal, o acesso de terceirizados a processos sigilosos; (ii) quais os requisitos mínimos para que o acesso seja considerado legítimo e seguro; e (iii) se há entendimento consolidado pela CGU sobre os limites e responsabilidades do órgão contratante nesse tipo de situação. É o relato.

4. ANÁLISE

4.1. A Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) estabelece em seu art. 6º que "cabe aos órgãos e entidades do poder público (...) assegurar a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso". A título de exemplo, o art. 23 prevê que são consideradas imprescindíveis à segurança da sociedade ou do Estado as informações cuja divulgação ou acesso irrestrito possam "prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas (inciso V)" ou às "atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações (inciso VIII)".

4.2. O art. 24 da LAI classifica as informações em três graus de sigilo: ultrassecreto, secreto e reservado, com prazos máximos de restrição de 25, 15 e 5 anos, respectivamente.

4.3. O art. 25, § 1º, da LAI diz que o acesso, a divulgação e o tratamento de informação classificada de sigilosa limitam-se às pessoas devidamente credenciadas na forma do regulamento com

necessidade de conhecê-la.

4.4. O Decreto nº 7.845, de 14 de novembro de 2012, regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo. O decreto condiciona o acesso a informações classificadas à demonstração de que o interessado necessita dessas informações para o exercício de seu cargo, função, emprego ou atividade, conforme se extrai, especialmente, dos arts. 12, 13 e 18.

> Decreto nº 7.845, de 14 de novembro de 2012.
>
> Art. 12. A concessão de credencial de segurança a uma pessoa fica condicionada aos seguintes requisitos:
>
> I - solicitação do órgão ou entidade pública ou privada em que a pessoa exerce atividade;
>
> II - preenchimento de formulário com dados pessoais e autorização para investigação;
>
> III - aptidão para o tratamento da informação classificada, verificada na investigação; e
>
> IV - declaração de conhecimento das normas e procedimentos de credenciamento de segurança e de tratamento de informação classificada.
>
> Art. 13. A habilitação para credenciamento de segurança e a concessão de credencial de segurança resultarão da análise objetiva dos requisitos previstos neste Decreto.
>
> [*omissis*]
>
> Art. 18. O acesso, a divulgação e o tratamento de informação classificada ficarão restritos a pessoas com necessidade de conhecê-la e que sejam credenciadas na forma deste Decreto, sem prejuízo das atribuições dos agentes públicos autorizados na legislação.
>
> Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, constante do Anexo I, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

4.5. No âmbito dos procedimentos correcionais, a Portaria Normativa CGU nº 27/2022 disciplina as fases de admissibilidade e os processos correcionais no Sistema de Correição do Poder Executivo Federal. Segundo os seus arts. 35 a 60, a fase de admissibilidade compreende o recebimento de denúncias, o juízo de admissibilidade e os procedimentos investigativos, incluindo a Investigação Preliminar Sumária (IPS).

4.6. Os procedimentos investigativos da Portaria Normativa CGU nº 27/2022 (Investigação Preliminar Sumária, Sindicância Investigativa e Sindicância Patrimonial) têm acesso restrito por força dos arts. 40, 46 e 50. Em razão das informações coletadas, é possível a classificação parcial ou integral dos autos nas categorias legais de sigilo.

4.7. Esta Coordenação-Geral já se manifestou sobre tema relacionado.

4.8. A Nota Técnica nº 1523/2021/CGUNE/CRG examinou a existência de restrição em relação ao cadastramento de dados no Sistema e-PAD por empregados terceirizados. Concluiu a CGUNE:

> 3.8. Depreende-se do rol de perfis no item 3.5 que compete ao Administrador atribuir perfil a cada usuário em consonância com as atividades a serem desempenhadas dentro do processo correcional, uma vez que o sistema busca justamente apoiar a atividade correcional e, como tal, todos os agentes que integram as unidades correcionais devem ter acesso ao EPAD, na medida dessas atribuições.
>
> 3.9. Assim, por exemplo, para um determinado usuário, a atribuição do perfil EPAD - Consulta pode ser suficiente, ao passo que outro agente, em razão da necessidade de inserção de peças no sistema para subsidiar o juízo de admissibilidade, necessite do perfil EPAD - Analista de juízo de admissibilidade. Todos os acessos e operações realizadas no sistema são registrados (artigo 9º), não sendo possível realizar qualquer operação no EPAD sem o prévio cadastramento como usuário pelo Administrador do sistema.

4.9. A questão do acesso de colaboradores terceirizados a informações sigilosas não encontra vedação expressa na legislação, desde que observados os requisitos legais.

4.10. O art. 2º, VII, do Decreto nº 7.845/2012 prevê que o credenciamento de segurança serve à habilitação de órgão ou entidade pública ou privada. Isso significa que a natureza do vínculo (estatutário, celetista, temporário ou terceirizado) não é, por si só, impeditiva do acesso a informações classificadas.

4.11. A legislação exige que (i) exista autorização legal (situação de agentes públicos); ou (ii) haja necessidade de conhecer a informação classificada com o respectivo credenciamento prévio (art. 18, *caput*, do Decreto nº 7.845/2012). Os requisitos do credenciamento constam do art. 12 do Decreto nº 7.845/2012.

4.12. Mesmo assim, o parágrafo único do art. 18 do Decreto nº 7.845/2012 institui a possibilidade de excepcionar as exigências acima. As pessoas sem credencial nem autorização legal têm a oportunidade de ser-lhes franqueado o acesso, desde que (i) possuam necessidade de conhecer as informações e (ii) assinem o "Termo de Compromisso de Manutenção de Sigilo - TCMS, constante do Anexo I, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei".

4.13. No caso dos colaboradores terceirizados que atuam em apoio administrativo à corregedoria, inserindo modelos de despachos em processos de admissibilidade e IPS, há que se avaliar se tal atividade configura efetiva necessidade de conhecer o conteúdo integral dos autos ou se pode ser realizada de forma segregada, com acesso apenas às informações estritamente indispensáveis.

4.14. A título exemplificativo, se o colaborador limita-se a inserir texto predefinido em um sistema, sem necessidade de análise do mérito ou do conteúdo fático do processo, pode-se estruturar o fluxo de trabalho de modo que o acesso seja restrito apenas aos dados necessários para a tarefa, sem visualização integral dos autos.

4.15. Por outro lado, se a atividade demanda leitura e compreensão do contexto dos autos para adequada inserção de despachos, haverá necessidade de conhecer, devendo-se, então, adotar as cautelas formais previstas na legislação.

4.16. Respondendo aos questionamentos formulados pelo INCRA, distinguem-se, para fins de definição dos requisitos mínimos de legitimidade e segurança do acesso de terceirizados, duas situações: (i) acesso a informações formalmente classificadas nos termos da Lei nº 12.527/2011 e do Decreto nº 7.845/2012; e (ii) acesso a informações sigilosas ou de acesso restrito, mas não formalmente classificadas nesses graus.

4.17. No primeiro caso, de informação classificada (graus reservado, secreto ou ultrassecreto), aplicam-se as seguintes balizas, extraídas do Decreto nº 7.845/2012:

- Demonstração da necessidade de acesso: a unidade competente deve motivar que o colaborador, em razão das atribuições que desempenha no órgão ou entidade, necessita conhecer a informação classificada para o exercício de suas atividades;
- Credencial de segurança: em regra, o acesso à informação classificada depende de que a pessoa esteja credenciada, na forma do Decreto nº 7.845/2012, observados os requisitos formais ali previstos para concessão de credencial;
- TCMS em caráter excepcional: se a pessoa não for credenciada nem autorizada por legislação específica e, ainda assim, for imprescindível permitir acesso pontual à informação classificada, admite-se, de modo excepcional, o acesso mediante assinatura de Termo de Compromisso de Manutenção de Sigilo, na forma do art. 18, parágrafo único, do Decreto nº 7.845/2012, com a devida motivação e controles reforçados.

4.18. Nessa hipótese, o termo de compromisso previsto no Decreto nº 7.845/2012 não se soma à credencial de segurança como requisito cumulativo ordinário, mas funciona como mecanismo excepcional para viabilizar acesso por pessoa que, por definição, não está credenciada nem autorizada por lei.

4.19. No segundo caso, mais frequente na realidade correcional, em que se trata de informação sigilosa ou de acesso restrito, mas não formalmente classificada nos graus da Lei nº 12.527/2011 e do Decreto nº 7.845/2012 (por exemplo, sigilo disciplinar previsto no art. 150 da Lei nº 8.112/1990, sigilo de documentos preparatórios e proteção da intimidade, honra e imagem nos termos da Lei nº 12.527/2011, e outros sigilos legais específicos), o regime aplicável é diverso. Nessa situação, não se exige credencial de segurança nos moldes do Decreto nº 7.845/2012, nem o TCMS ali previsto, porém convém a observância, no mínimo, dos seguintes parâmetros:

- Demonstração da necessidade de acesso: o órgão deve justificar, de forma motivada,

que o acesso do colaborador terceirizado é indispensável ao desempenho das atribuições previstas no contrato de prestação de serviços e que não é possível organizar o trabalho de modo a dispensar ou reduzir esse acesso;

- Formalização mediante termo de confidencialidade contratual ou interno: é recomendável que o contrato com a empresa prestadora de serviços contenha cláusulas de confidencialidade, proteção de dados e responsabilização por eventual vazamento ou uso indevido de informações, e que cada colaborador terceirizado com acesso a procedimentos sigilosos assine termo de confidencialidade individual, no qual se explicitem os deveres de sigilo, o escopo das informações protegidas e as consequências administrativas, civis e penais do descumprimento;
- Registro e controle de acesso: o órgão deve manter registro dos acessos realizados, preferencialmente por meio de sistema eletrônico que permita auditoria posterior, de modo a possibilitar a identificação de quem consultou ou manipulou cada processo ou documento;
- Supervisão e validação por servidor: é essencial que todo documento inserido ou manipulado por terceirizado seja objeto de checagem e validação final por servidor público responsável pela análise de mérito, que responderá pelos atos praticados nos autos;
- Segregação de funções, sempre que possível: recomenda-se estruturar os fluxos de trabalho de modo a minimizar o acesso irrestrito de terceirizados, permitindo-lhes visualizar apenas as informações estritamente necessárias ao cumprimento de suas tarefas de apoio;
- Limitação e revisão periódica de perfis de acesso em sistemas: os perfis concedidos a colaboradores terceirizados em sistemas informatizados devem ser restritos ao mínimo necessário e objeto de revisão periódica, de forma a evitar ampliações indevidas de acesso por mera inércia administrativa.

4.20. Nessa segunda hipótese, o termo de confidencialidade de natureza contratual ou interna não substitui qualquer requisito legal eventualmente aplicável, mas assume papel central como instrumento de gestão de risco e de explicitação de deveres, sobretudo quando o sigilo decorre de dispositivos como o art. 150 da Lei nº 8.112/1990, do art. 7º, § 3º, e do art. 31 da Lei nº 12.527/2011, bem como de normas correcionais específicas.

4.21. Quanto às responsabilidades do órgão contratante, a Administração continua responsável pela adequada gestão das informações sob sua custódia, devendo: (i) avaliar a real necessidade de acesso do terceirizado em cada situação; (ii) adotar medidas de segurança da informação proporcionais ao grau de sensibilidade dos dados; (iii) definir com clareza as atividades que podem ser desempenhadas por colaboradores terceirizados e as que são privativas de servidores; (iv) supervisionar a atuação desses colaboradores; e (v) apurar e responsabilizar eventuais vazamentos ou usos indevidos, tanto na esfera interna (eventuais falhas de servidores) quanto na contratual, civil e penal, conforme o caso.

4.22. O colaborador terceirizado, por sua vez, sujeita-se às sanções contratuais previstas no instrumento de contratação, podendo responder também nas esferas cível e penal por danos decorrentes de violação de sigilo, sem prejuízo de eventual responsabilização da empresa contratada, na forma do contrato e da legislação aplicável.

5. CONCLUSÃO

5.1. Ante o exposto, conclui-se que:

a) Não há vedação legal ao acesso de colaboradores terceirizados a processos correcionais sigilosos (Juízo de Admissibilidade e IPS), desde que observados os requisitos da Lei nº 12.527/2011 e do Decreto nº 7.845/2012;

b) O acesso deve ser condicionado à demonstração da necessidade de conhecer, inerente ao efetivo exercício das atribuições contratuais do colaborador, independentemente de vínculo;

c) Se a informação estiver formalmente classificada em grau de sigilo (reservado, secreto ou ultrassecreto), é necessária a concessão de credencial de segurança no grau correspondente, nos termos do Decreto nº 7.845/2012;

d) O termo de confidencialidade é instrumento complementar relevante, mas não substitui a credencial de segurança quando esta for exigível;

e) Recomenda-se que o órgão adote medidas de segregação de funções, controle de acesso, supervisão por servidor efetivo e registro de acessos, a fim de assegurar a proteção da informação e a rastreabilidade de eventuais incidentes;

f) O órgão responde pela adequada gestão das informações sigilosas sob sua custódia, devendo avaliar a real necessidade de acesso e adotar cautelas proporcionais ao grau de sensibilidade dos dados;

g) No caso específico do INCRA, se as atividades dos terceirizados limitam-se à inserção mecânica de modelos de despacho, sem necessidade de análise de mérito, é conveniente a estruturação do fluxo de trabalho de modo a minimizar o acesso ao conteúdo integral dos autos, assegurando-se a validação final por servidor efetivo.

5.2. Por fim, submeto a presente Nota Técnica à consideração do Sr. Coordenador-Geral de Uniformização de Entendimentos desta Corregedoria-Geral da União.

5.3. À consideração superior.

Documento assinado eletronicamente por **JOAO VICTOR IOSCA VIERO**, **Auditor Federal de Finanças e Controle**, em 23/04/2026, às 15:57, 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://super.cgu.gov.br/conferir informando o código verificador 3925434 e o código CRC 610F77A0

Referência: Processo nº 00190.110340/2025-14 SEI nº 3925434

CONTROLADORIA-GERAL DA UNIÃO

DESPACHO CGUNE

1. Aprovo a Nota Técnica n° 29/2026/CGUNE/DICOR/CRG.

2. Encaminho o processo à consideração superior do Diretor de Articulação, Monitoramento e Supervisão do Sistema de Correição do Poder Executivo Federal.

Documento assinado eletronicamente por **BRUNO WAHL GOEDERT**, **Coordenador-Geral de Uniformização de Entendimentos**, em 23/04/2026, às 16:20, 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://super.cgu.gov.br/conferir informando o código verificador 4057563 e o código CRC EF332422

Referência: Processo nº 00190.110340/2025-14 SEI nº 4057563

CONTROLADORIA-GERAL DA UNIÃO

DESPACHO DICOR

Estamos de acordo com a Nota Técnica 29 (3925434) da CGUNE e como o Despacho CGUNE (4057563) de 23/04/2026.

Informamos que somos favoráveis a fixação das seguintes teses:

1. Não há vedação legal ao acesso de colaboradores terceirizados a processos correcionais sigilosos (Juízo de Admissibilidade e IPS), desde que observados os requisitos da Lei nº 12.527/2011 e do Decreto nº 7.845/2012;
2. O acesso deve ser condicionado à demonstração da necessidade de conhecer, inerente ao efetivo exercício das atribuições contratuais do colaborador, independentemente de vínculo;
3. Se a informação estiver formalmente classificada em grau de sigilo (reservado, secreto ou ultrassecreto), é necessária a concessão de credencial de segurança no grau correspondente, nos termos do Decreto nº 7.845/2012;
4. O termo de confidencialidade é instrumento complementar relevante, mas não substitui a credencial de segurança quando esta for exigível;
5. Recomenda-se que o órgão adote medidas de segregação de funções, controle de acesso, supervisão por servidor efetivo e registro de acessos, a fim de assegurar a proteção da informação e a rastreabilidade de eventuais incidentes;
6. O órgão responde pela adequada gestão das informações sigilosas sob sua custódia, devendo avaliar a real necessidade de acesso e adotar cautelas proporcionais ao grau de sensibilidade dos dados; e
7. No caso específico do INCRA, se as atividades dos terceirizados limitam-se à inserção mecânica de modelos de despacho, sem necessidade de análise de mérito, é conveniente a estruturação do fluxo de trabalho de modo a minimizar o acesso ao conteúdo integral dos autos, assegurando-se a validação final por servidor efetivo.

Encaminhem-se os autos à CRG para avaliação, e caso considere pertinente, adoção das demais providências de sua competência.

Documento assinado eletronicamente por **ADRIANO AUGUSTO DE SOUZA**, **Diretor de Articulação, Monitoramento e Supervisão do Sistema de Correição do Poder Executivo Federal**, em 23/04/2026, às 16:46, 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://super.cgu.gov.br/conferir informando o código verificador 4057750 e o código CRC D40067F1

Referência: Processo nº 00190.110340/2025-14 SEI nº 4057750

CONTROLADORIA-GERAL DA UNIÃO

DESPACHO CRG

1. De acordo com a Nota Técnica n° 29/2026/CGUNE/DICOR/CRG (3925434), aprovada pelos Despachos CGUNE (4057563) e DICOR (4057750).

2. Encaminhe-se à CGUNE para divulgação à consulente e para inclusão na Base de Conhecimento da CGU.

Documento assinado eletronicamente por **FERNANDA ALVARES DA ROCHA**, **Corregedora-Geral da União**, em 27/04/2026, às 10:08, 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://super.cgu.gov.br/conferir informando o código verificador 4057833 e o código CRC ECB39D21

Referência: Processo nº 00190.110340/2025-14 SEI nº 4057833