



Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA

Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, NATAL / RN, CEP 59015-300

Fone: (84) 4005-0768, (84) 4005-0750

PARECER Nº 6/2024 -
EDP/IFRN/RE/IFRN

15 de outubro de 2024

PARECER TÉCNICO DO ENCARREGADO DE DADOS PESSOAIS DO IFRN E DA AUTORIDADE DE MONITORAMENTO DA LEI DE ACESSO À INFORMAÇÃO E PROTOCOLO PARA DIVULGAÇÃO DE INFORMAÇÕES RELACIONADAS A PROCESSOS CORRECIONAIS E DEMAIS PROCESSOS QUE TENHAM RESTRIÇÃO EM RAZÃO DA EXISTÊNCIA DE DADOS PESSOAIS

Assunto: Protocolo a ser seguido para a divulgação das informações, bem como sobre quais são os servidores, setores ou autoridades expressamente autorizados a proceder com a divulgação de dados não sensíveis em processos de apuração de responsabilidade ou com alteração de níveis de acesso de processos em geral, em conformidade a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) e com a Lei de Acesso à Informação (LAI - Lei nº 12.527/2011).

Interessado(s): IFRN; Gabinete da Reitoria; Serviço de Informação ao Cidadão no âmbito do IFRN; [REDACTED]

Data: (mesma data da assinatura eletrônica)

Encarregado de Dados Pessoais: Ismael Felix Coutinho Neto, [Portaria nº 1859/2023 - RE/IFRN](#).

1. Introdução e contextualização

1.1. Introdução e objetivo

Este parecer tem como objetivo avaliar a conformidade das práticas de tratamento de dados pessoais do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN) com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e com a Lei de Acesso à Informação (LAI - Lei nº 12.527/2011). Além disso, visa fornecer recomendações para adequação às exigências legais quanto ao protocolo a ser seguido para a divulgação das informações; bem como sobre quais são os servidores, setores ou autoridades expressamente autorizadas a proceder com a divulgação de dados não sensíveis em processos de apuração de responsabilidade ou com alteração de níveis de acesso de processos em geral.

A LGPD apresenta normas referentes ao tratamento de dados pessoais, inclusive nos meios digitais, realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Por sua vez, a LAI estabelece procedimentos com a finalidade de garantir o acesso a informações, visando garantir o direito fundamental de receber dos órgãos públicos informação de interesse particular, coletivo ou geral, "mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão" (Art. 5º, da Lei nº 12.527/2011).

Nesse sentido, para fins de orientação, no desenvolvimento deste parecer, são observados normativos, guias e enunciados dos órgãos centrais responsáveis por regular e garantir a implementação da legislação informada, quais sejam a Autoridade Nacional de Proteção de Dados e a Controladoria Geral da União, além dos dispositivos previstos na Política de Privacidade e Proteção de Dados do IFRN.

1.2. Contexto

Trata-se do encaminhamento do processo 23057.006702.2024-22, realizado pelo Senhor Reitor do IFRN, acolhendo a "NOTA n. 00075/2024/PF-IFRN/PFIFRIO GRANDE DO NORTE/PGF/AGU, por seus próprios fundamentos".

O processo apresenta no campo assunto: "Requerimento Nº 002/2024/REGIF-CNAT à Comissão Eleitoral Local do IFRN/CNAT". No entanto, ao analisar o requerimento, de forma mais específica, o processo trata do requerimento para "alteração do nível de acesso do tipo "restrito" para o tipo "público"" de processos que se referem a denúncias

relacionadas a servidores públicos do IFRN, no período anterior e durante a campanha eleitoral do IFRN.

No que concerne ao mérito do requerimento no campo técnico-jurídico quanto à análise da viabilidade de conceder acesso público a processos relativos a denúncias em trânsito ou concluídos, já foi devidamente avaliado pela Procuradoria Jurídica do IFRN, através da NOTA n. 00075/2024/PF-IFRN/PFIFRIO GRANDE DO NORTE/PGF/AGU, acolhida pelo Sr. Reitor.

Para fins de contextualizar esse parecer, extrai-se da Nota jurídica já informada:

"compreende-se que durante o período da apuração até o julgamento, os processos envolvendo denúncias devem permanecer sigilosos. Uma vez julgados ou encerrados por outras razões, como por exemplo, a falta de materialidade, poderão ser publicizados os dados não sensíveis ou que não necessitem permanecer em sigilo com fundamento em outras hipóteses legais."

e

"Recomenda-se proceder consulta ao Encarregado pelo Tratamento de Dados Pessoais (art. 41 da Lei Geral de Proteção de Dados Pessoais) designado pelo IFRN acerca do protocolo a ser seguido para a divulgação das informações, bem como sobre quais são os servidores, setores ou autoridades expressamente autorizados a proceder com a divulgação de dados não sensíveis em processos de apuração de responsabilidade ou com alteração de níveis de acesso de processos em geral."

Dessa forma, estando resolvida a questão do sigilo/restrrição do processo ao público em geral relacionado a processos que envolvem denúncias relativas a servidores públicos, caberá a este Encarregado de Dados Pessoais promover a análise de riscos relacionada ao objeto do contexto informado e adotar as providências relativas à definição de um protocolo quanto a divulgação de dados não sensíveis em processos de apuração de responsabilidade, tratando da necessidade de indicar de quem é atribuição de promover a alteração de níveis de acesso desse tipo de processo e de processos em geral.

2. Dos subsídios/contexto para o gerenciamento de riscos a partir das práticas de tratamento de dados pessoais adotadas pelo IFRN no tratamento de processos que envolvem denúncia e de processos correccionais

2.1. Coleta de dados

2.1.1. Descrição das práticas de coleta de dados.

A coleta de dados pessoais no que se refere a processos que envolvem denúncias e que podem ou não se transformar em processos correccionais, atualmente é realizada por meio da plataforma integrada de ouvidoria e acesso à informação FALA.br.

Isso ocorre por meio de escuta realizada pela Ouvidoria do IFRN ou quando a denúncia é realizada de forma espontânea a chefias e servidores diversos da instituição. Esses servidores, por vezes, orientam ao denunciante que registre os fatos no FALA.br, que serão atendidos pela Ouvidoria do IFRN, ou registram em documentos oficiais, que serão tramitados por meio de processo eletrônico, informando qual o tipo de acesso no Sistema Unificado de Administração Pública (SUAP).

2.1.2. Descrição dos dados coletados:

São dados pessoais, sensíveis ou não, coletados por meio do processo de denúncia em relação a servidores do IFRN, que são objeto de análise:

- dados de identificação, endereço e contato do denunciante;
- dados de identificação, endereço e contato e/ou dados pessoais diversos que podem levar a identificação de um servidor que precise ser investigado em uma denúncia;
- dados de identificação, endereço e contato de pessoas que são intimadas como testemunhas, declarantes, informantes e que de alguma forma precisam participar do processo correccional;
- dados de identificação dos membros e secretários de comissões de processos correccionais; e
- informações sensíveis ou não, como o contexto, local da ocorrência e demais elementos probatórios que identificam o denunciante, o denunciado ou outro servidor que possa ser identificado.

2.1.3. Avaliação da conformidade com os princípios da LGPD, acerca da coleta dos dados:

Considerando os princípios da finalidade, adequação e necessidade, que se referem ao propósito legítimo do tratamento, à compatibilidade desse tratamento com as finalidades legítimas e informadas aos titulares, e à limitação do tratamento ao mínimo necessário para atendimento à finalidade, não se vislumbra não conformidade com a LGPD. Isso ocorre porque

a coleta e o tratamento dos dados pessoais são necessários para o cumprimento da Lei 8.112/90, que é uma obrigação regulatória do controlador. Além disso, esses procedimentos estão alinhados com normativos, manual e sistemas do órgão central de correição do Governo Federal, cabendo ao IFRN dar o cumprimento devido.

Considerando o livre acesso como garantia aos titulares dos dados pessoais, de consulta facilitada e gratuita sobre a forma e a duração do tratamento e sobre a integralidade de seus dados pessoais; considerando, ainda, que as informações repassadas a esses titulares sobre o sigilo do processo e que podem ter acesso aos documentos que foram produzidos com a sua participação; e considerando, por fim, que, no caso do denunciado, ele tem acesso ao inteiro teor do processo, por uma obrigação legal; percebe-se de forma clara o cumprimento da LGPD em atenção aos princípios do livre acesso, da qualidade dos dados e da transparência dos dados.

Com relação à segurança, as medidas restritivas implementadas nos sistemas do governo federal e do IFRN garantem que os documentos que contêm restrição de acesso sejam acessíveis apenas aos interessados legítimos, demonstrando adequação à LGPD. O princípio da prevenção está devidamente interligado à segurança, assegurando a conformidade dos procedimentos.

No entanto, um ponto de atenção merece destaque e pode ser aperfeiçoado. Quando processos são encaminhados para as autoridades responsáveis por decisões, servidores de setores de gabinete e secretarias também têm livre acesso a esses documentos. Embora a Lei 8.112/90 exija sigilo em relação às informações da repartição, isso, por si só, não configura um procedimento de segurança eficaz para essas informações.

Dessa forma, para melhor atender os princípios de segurança e prevenção, o módulo de processo eletrônico deverá passar por ajustes para que apenas servidores formalmente designados e capacitados tenham acesso a processos que guardem algum tipo de restrição de acesso em razão da legislação, como é o caso do processo que é objeto de análise.

Em relação ao princípio da não discriminação, a restrição ao processo garante que as informações pessoais sejam utilizadas apenas para fins legítimos. Dessa forma, não se observa ausência de conformidade com o princípio da não discriminação, que impede o tratamento de dados para fins discriminatórios, ilícitos ou abusivos.

Por fim, em relação ao princípio da responsabilização e prestação de contas, é necessário considerar a fragilidade parcial da estrutura responsável por processos correcionais. O IFRN precisa ampliar seus esforços para demonstrar a adoção de medidas eficazes que comprovem a observância e o cumprimento das normas de proteção de dados pessoais nessa área.

2.2. Compartilhamento de Dados

2.2.1. Descrição e avaliação dos tipos de tratamento relacionados ao processamento e ao compartilhamento de dados pessoais em processos institucionais:

a) Processamento: classificação (maneira de ordenar os dados conforme algum critério estabelecido), utilização (ato ou efeito do aproveitamento dos dados), reprodução (cópia de dado preexistente obtido por meio de qualquer processo), processamento, avaliação (analisar o dado com o objetivo de produzir informação) ou controle da informação (ação ou poder de regular, determinar ou monitorar as ações sobre o dado), extração (ato de copiar ou retirar dados do repositório em que se encontrava) e modificação (ato ou efeito de alteração do dado) de dados pessoais.

Em relação ao processamento de dados pessoais, para a finalidade que se destina este parecer será avaliada apenas a classificação.

No Sistema Unificado de Administração Pública (SUAP), os documentos e processos são classificados de acordo com a base legal específica para cada caso, sendo a Lei de Acesso à Informação, uma das bases mais utilizadas no IFRN para restringir o acesso a documentos e processos eletrônicos, uma vez que o Artigo 31 apresenta que "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" e o Inciso 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".

Observando o SUAP, percebe-se que o sistema não realiza qualquer crítica dirigida ao usuário quando ele realiza essa classificação, de maneira tal que o usuário realiza o procedimento sem, por vezes, compreender a importância dessa ação para o comprometimento institucional com a ausência de transparência relacionada a seus processos e com a falta de zelo com os direitos fundamentais garantidos ao cidadão. Desse contexto, extrai-se que há uma certa fragilidade institucional relacionada à transparência de seus processos, sendo necessário instituir um plano de ação para aperfeiçoar o processo de classificação de documentos.

b) Compartilhamento: transmissão (movimentação de dados entre dois pontos por meio de dispositivos eletrônicos, telefônicos); comunicação (transmitir informações pertinentes a políticas de ação sobre os dados); e compartilhamento

de dados pessoais;

Nessa seção, analisado apenas tratamento de compartilhamento de dados pessoais, o qual se dá por meio dos documentos e processos institucionais, através da transmissão desses por meio digital.

No IFRN, essa transmissão se dá por meio do SUAP e o compartilhamento da dados pessoais, por meio do trâmite desses processos. Em regra, processos com restrição de acesso são compartilhados via SUAP e passíveis de acesso apenas pelos servidores do setor o qual o processo é encaminhado.

Uma fragilidade encontrada nesse processo é o fato de que todos os servidores do setor o qual o processo foi encaminhado, tem acesso irrestrito ao processo, sem que haja nenhum aviso ou necessidade de assinatura de ciência por parte do servidor que acessa. Entretanto, é possível se ter o controle de acesso, uma vez que o próprio sistema promove o registro dos acessos.

2.3. Avaliação das medidas de segurança da informação adotadas, relacionadas ao armazenamento e segurança dos dados:

De acordo com o Plano de Integridade do IFRN, são medidas de segurança da informação implementadas pela área de tecnologia da informação e comunicação do IFRN, a fim de garantir a integridade dos dados:

- sistemas desenvolvidos e recursos tecnológicos utilizados com base em Controle de Acesso Baseado em Funções (RBAC).
- sistemas desenvolvidos e recursos tecnológicos utilizando Criptografia de Dados
- acesso a sistemas e recursos baseado no conceito de menor privilégio possível
- ferramentas de monitoramento em Tempo Real
- apoio da Secretaria de Governo Digital/MGI na implementação do Programa de Privacidade e Segurança da Informação (PPSI)
- políticas de Gerenciamento de Senhas e Políticas de Senhas Fortes;
- implementação de mecanismos em ativos de rede e estações de trabalho, voltadas a proteção contra Malware e outros tipos de ameaças; e
- controle de Acesso a Documentos Físicos e Digitais.

Tendo em vista os controles já implementados pela área de Tecnologia da Informação e Comunicação (TIC) do IFRN, percebe-se que a instituição busca garantir a proteção dos dados custodiados pela Instituição. No entanto, é importante considerar o contexto geral de conformidade com os princípios, incluindo eventuais fragilidades que possam comprometer a segurança dos dados e a prevenção, conforme foi apresentado na seção 2.1.3. deste parecer.

3. Identificação de Riscos e construção de protocolo para sanear-los

3.1. Riscos relacionados à proteção de dados pessoais

Em relação aos dispositivos preventivos e de segurança e ao próprio tratamento de dados pessoais em suas várias fases, como identificadas no nas seções 2.1, 2.2 e 2.3 deste parecer, identificam-se alguns riscos que precisam de especial atenção para que não ocorram, como:

- vazamento de dados pessoais de denunciantes;
- vazamento de dados pessoais de vítimas e informantes presentes em processos correcionais;
- vazamento de dados pessoais do acusado, quando o mesmo não foi considerado culpado no processo;
- vazamento de dados pessoais de testemunhas; e
- vazamento de dados pessoais de outros envolvidos ou citados em processos correcionais.

Até o presente momento, a instituição não dispõe registro oficial de indicador que trate da ocorrência desses riscos. Uma eventual ocorrência pode causar prejuízo significativo ao processo que envolve algum tipo de denúncia; trazer grandes danos à imagem, honra e intimidade dos titulares de dados envolvidos; e diversos outros efeitos adversos decorrentes de um eventual vazamento de dados pessoais. Além disso, pode resultar em sanções para quem causou o vazamento e danos à imagem do IFRN, não sendo essa uma lista exaustiva.

3.2. Riscos relacionados à Lei de Acesso à Informação

Abordando a Lei de Acesso à Informação, conforme visto na Nota da Procuradoria Federal junto ao IFRN nº 00075/2024/PF-IFRN/PFIFRIO GRANDE DO NORTE/PGF/AGU, não há prejuízo à transparência quando há restrição de acesso informada em processo de denúncia de caráter sigiloso, enquanto este não tiver sido devidamente julgado pela autoridade competente.

Considerando agora um processo julgado, os riscos informados em relação à proteção de dados pessoais continuam válidos. No entanto, nesse novo momento, devem ser considerados os riscos quanto à transparência e ao acesso à informação, quais sejam:

- comprometimento do direito fundamental de acesso à informação do cidadão;
- comprometimento dos níveis de transparência ativa e passiva da instituição;
- ateste de não conformidade com a Lei de acesso à informação por parte do órgão central que regula a integridade, a transparência e o acesso à informação; e
- comprometimento da imagem institucional perante os cidadãos e perante a comunidade acadêmica.

Como consequência da ocorrência desses riscos, podem surgir conflitos internos e externos no campo administrativo e judicial. Além disso, pode resultar em processos de responsabilização para aqueles que deram causa aos riscos, negatização do conceito da instituição perante órgãos de auditoria interna e externa, e auditorias do órgão de controle externo. Essas auditorias podem resultar na responsabilização de autoridades e servidores que não observaram a conformidade legal.

4. Conclusão

Este parecer técnico conclui que o IFRN está parcialmente, em menor parte, em conformidade com a Lei de Acesso à Informação e, consequentemente, com a Lei de Proteção de Dados Pessoais, tratando-se do procedimento de classificação e trâmite de processos com restrição de acesso previstos na lei, uma vez que os mecanismos de transparência que hoje existem não promovem a interlocução dos dois diplomas legais de forma complementar, permitindo a existência de uma certa fragilidade institucional quanto a necessidade de promover o atendimento aos direitos fundamentais que garantem ao cidadão de dispor das informações não sigilosas tuteladas pelo IFRN, com o devido respeito à proteção dos seus dados pessoais.

É importante, ainda, apresentar o que traz o enunciado 12/2023, da Controladoria Geral da União:

"O fundamento "informações pessoais" não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados, etc) para que, devidamente protegidos, o restante dos documentos ou processos solicitados sejam fornecidos. Além disso, a proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, podendo aquela ser flexibilizada quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser, nos termos do art. 31, § 3º, inciso V da Lei nº 12.527/2011."

Por fim, a fim de promover as melhorias necessárias à transparência institucional e à proteção de dados pessoais, faz-se necessário a implementação das medidas sugeridas por ocasião da análise de riscos e dos processos de tratamento, itens 2 e 3 deste parecer, e da apresentação dos protocolos que tratam do compartilhamento de documentos e/ou processos que contenham informações pessoais e outras informações protegidas por sigilo legal, especialmente aqueles que tratam da área correcional, para assim garantir a plena conformidade com as legislações e normativos amplamente discutidos neste parecer.

Diante do exposto, será apresentada, anexo a este Parecer, a minuta de Protocolo que trata do acesso à informação relacionada a processos que tenham sido classificados com algum tipo de restrição em razão da existência de dados pessoais em seus documentos.

A N E X O

PROTOCOLO PARA DIVULGAÇÃO DE INFORMAÇÕES RELACIONADAS A PROCESSOS CORRECIONAIS E DEMAIS PROCESSOS QUE TENHAM RESTRIÇÃO EM RAZÃO DA EXISTÊNCIA DE DADOS PESSOAIS

Protocolo a ser seguido para a divulgação das informações, bem como sobre quais são os servidores, setores ou autoridades expressamente autorizados a proceder com a divulgação de dados não sensíveis em processos de apuração de responsabilidade ou com alteração de níveis de acesso de processos em geral

1. INTRODUÇÃO

Este protocolo tem o objetivo de orientar os setores do IFRN a como proceder diante da necessidade de divulgar informações contidas em documentos e/ou processos institucionais. Para tanto, essas orientações se apresentam na forma de um fluxograma acerca do tratamento do processo de divulgação de informações, observando os princípios apresetados na Lei de Acesso à Informação e na Lei Geral de Proteção de Dados Pessoais, especialmente o princípio do

interesse público, da eficiência, da LAI e os princípios da finalidade e da necessidade, da LGPD.

Esse fluxograma irá atender ao disposto na Nota. 00075/2024/PF-IFRN/PFIFRIO GRANDE DO NORTE/PGF/AGU, aprovada pelo Senhor Reitor do IFRN, acerca da necessidade de instituir um protocolo a ser seguido para a divulgação das informações, bem como sobre quais são os servidores, setores ou autoridades expressamente autorizados a proceder com a divulgação de dados não sensíveis em processos de apuração de responsabilidade ou com alteração de níveis de acesso de processos em geral.

2. BASE LEGAL

- Lei nº 8.112/1990: dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
- Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI): dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no [inciso XXXIII do art. 5º](#), no [inciso II do § 3º do art. 37](#) e no [§ 2º do art. 216 da Constituição Federal](#);
- Lei nº 13.460/2017: dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública;
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD): dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;
- Lei nº 13.608/2018: dispõe sobre o serviço telefônico de recebimento de denúncias e sobre recompensa por informações que auxiliem nas investigações policiais; e altera o art. 4º da Lei nº 10.201, de 14 de fevereiro de 2001, para prover recursos do Fundo Nacional de Segurança Pública para esses fins;
- Lei 9.784/1999: Regula o processo administrativo no âmbito da Administração Pública Federal;
- Decreto 7.724/2012: regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do **caput** do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;
- Decreto nº 10.153/2019: salvaguardas de proteção à identidade dos denunciantes;
- Decreto nº 9.492/2018: institui o Sistema de Ouvidoria do Poder Executivo federal...;
- Decreto 11.529/2023: institui o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal;
- Parecer nº 00101/2022/PF-IFRN/PFIFRIO GRANDE DO NORTE/PGF/AGU: sobre a competência de instaurar processos correccionais no âmbito do IFRN;
- Nota Técnica nº 2418/2023/CGUNE/DICOR/CRG: disponibilização de acesso aos processos administrativos disciplinares finalizados;
- Manual de Processo Administrativo Disciplinar (CGU, 2022);
- Guia de Transparência Ativa (GTA) para órgãos e entidades do Poder Executivo Federal: um compilado de disposições normativas, elaborado pela Controladoria-Geral da União (CGU), com o objetivo de auxiliar no correto cumprimento das obrigações de transparência ativa.

3. PROTOCOLO

O protocolo a ser seguido para a divulgação das informações deve especificar quais servidores, setores ou autoridades estão expressamente autorizados a divulgar dados não sensíveis em processos de apuração de responsabilidade ou a alterar os níveis de acesso de processos em geral.

3.1. Considerações sobre processos sem restrição ou ostensivos, restritos e processos sigilosos.

As informações sob a guarda do IFRN, assim como em outros órgãos e entidades da Administração Pública são, em geral, públicas. O tratamento dessas informações deve ser restrito apenas em casos em que a lei especificar. Dito isso, tem-se que informações públicas produzidas ou mantidas pelo IFRN podem ser acessadas ou estar disponíveis a qualquer cidadão, desde que não se enquadrem nas exceções previstas na Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI) e em outras legislações vigentes, incluindo a Lei Geral de Proteção de Dados (LGPD).

Como exceções à regra de acesso à informação temos:

- Informações Pessoais (restrição prevista pela LAI e pela LGPD): são informações relacionadas a uma determinada pessoa ou que possam identificá-la. Seu tratamento deve respeitar a intimidade, vida privada, honra e a imagem, bem como as liberdades e garantias individuais. As informações pessoais não são públicas e terão seu acesso restrito. Elas podem ser acessadas pelos agentes públicos legalmente autorizados e pela pessoa a que elas se referirem. O tratamento dessas informações pessoais é disciplinado na LGPD, conforme disposições contidas

principalmente nos artigos 7º, 11, 14 e 23, da LGPD;

- Informações restritas com base em outras leis: são informações protegidas por outras legislações, tais como o sigilo bancário, fiscal, comercial, empresarial e segredo de justiça, assim como informações relativas à investigação de responsabilidade de servidor ou discente;
- Informações classificadas como sigilosas: são aquelas cuja divulgação possa colocar em risco a segurança da sociedade (vida, segurança, saúde da população) ou do Estado (soberania nacional, relações internacionais, atividades de inteligência). Por isso, apesar de serem públicas, o acesso a elas deve ser restringido por meio da classificação prévia pela autoridade competente.
- Informações pessoais: são as informações relacionadas à pessoa natural identificada ou identificável, podendo ainda ser considerada como sensíveis aquelas informações que tratem 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. Essas informações terão seu acesso restrito a agentes públicos legalmente autorizados e a pessoa a que se referirem, independentemente de classificação de sigilo, pelo prazo máximo de cem anos a contar da data de sua produção.

Dessa forma, os documentos são classificados em três grupos, de acordo com a natureza das suas informações:

- Documento sem restrição de acesso ou ostensivo: regra comum para documentos públicos. São aqueles cujo teor deve ser de conhecimento do público em geral e deve ser disponibilizado para consulta sem restrições, atendendo ao princípio do interesse público;
- Documento restrito: é aquele cujo teor não deve ser do conhecimento do público em geral, sendo acessados apenas pelos interessados e por agentes públicos das unidades nas quais são tramitados, atendendo os princípios da finalidade e da necessidade;
- Documento sigiloso: documento que requer rigorosas medidas de segurança e cujo teor deve ser, exclusivamente, do conhecimento de pessoas credenciadas, ou seja, agentes públicos diretamente ligados à sua análise.

A LAI apresenta, em seu Artigo 24:

"Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.

§ 1º Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no **caput**, vigoram a partir da data de sua produção e são os seguintes:

I - ultrassecreta: 25 (vinte e cinco) anos;

II - secreta: 15 (quinze) anos; e

III - reservada: 5 (cinco) anos."

Esse tipo de documento deve ser classificado somente por autoridades com competência para tal. O IFRN não possui, no momento, classificação de suas informações em grau de sigilo (ultrassecreto, secreto e reservado).

Portanto, atualmente, os documentos produzidos pelo IFRN poderão somente ser considerados ostensivos ou restritos, de acordo com a natureza das informações disponíveis. Os pedidos de acesso à informação dos documentos sob guarda ou produzidos pelo IFRN deverão ser feitos ao Serviço de Informação ao Cidadão, preferencialmente, por meio da Plataforma Integrada de Ouvidoria e Acesso à Informação, Fala.BR, disponível no link <https://falabr.cgu.gov.br/web/home>, ou acessados por meio da página de acesso à informação do IFRN, quando disponibilizadas, no endereço eletrônico: <https://portal.ifrn.edu.br/acesso-a-informacao/>.

3.2. Competências para a divulgação de informações não classificadas com ou sem restrição contidas em processos institucionais.

- O setor competente para identificar se há elementos mínimos de relevância, autoria e materialidade em um processo de denúncia no IFRN é a Ouvidoria do IFRN, podendo arquivar um processo mesmo antes de ser apreciado pela autoridade máxima da instituição. Esse tipo de processo, quando arquivado pela Ouvidoria, deverá ser considerado para todos os efeitos, um processo público, desde que provido o seu tratamento à luz da Lei Geral de Proteção de Dados Pessoais e demais legislações que tratem de sigilo processual, zelando pela proteção do denunciante e de todas demais pessoas citadas no processo;
- A autoridade competente para instaurar e julgar processo de denúncia acerca de um servidor público é o Dirigente Máximo do IFRN. A Lei retira a restrição de forma automática do processo tido como julgado, devendo ser preservados os dados pessoais que possam levar a identificação das pessoas envolvidas com o processo, a exceção

do(s) servidor(s) apenados no processo, observando, ainda, nesse caso o princípio da finalidade e do interesse público;

- Processos correccionais em andamento têm o seu sigilo garantido pelo Art. 150, da Lei 8.112/1990, sendo, portanto, competentes para assegurar o sigilo legal do processo, todos os que têm acesso ao seu conteúdo;
- O Reitor do IFRN e, de forma delegada, o Chefe da Unidade Setorial do SISCOR, são as autoridades competentes para aprovar a versão resumida de um processo correccional julgado a ser disponibilizada em transparência ativa e aprovar disponibilização de versão integral do processo julgado em transparência passiva (mediante resposta à solicitação de acesso à informação), com atenção à proteção de dados pessoais, dados pessoais sensíveis e demais informações protegidas por sigilo legal. Deverá ser observado o que dispõe a Nota Técnica nº 2418/2023/CGUNE/DICOR/CRG;
- O Chefe da Unidade Setorial do SISCOR é o servidor competente para aprovar alterações de grau de restrição de documentos incluídos em processos correccionais concluídos;
- O chefe do setor que tem a guarda de processos que foram classificados em desconformidade com a Lei como processos restritos é o servidor competente para promover a alteração quanto à restrição do processo;
- O servidor designado como autoridade de monitoramento da Lei de Acesso à Informação é competente para atestar a não conformidade de processos e documentos com a Lei de Acesso à Informação;
- O servidor designado como Encarregado de Dados Pessoais é competente para atestar a não conformidade de processos e documentos com a Lei de Proteção de Dados Pessoais, devendo ter atenção especial quanto ao princípio do interesse público e da finalidade no processo de análise, resguardando contudo, os dados que, se divulgados, comprometam o direito fundamental à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas;
- É competente para promover a divulgação em transparência ativa dos processos sem restrição de acesso, especialmente os processos de que tratam o Guia de Transparência Ativa da Controladoria Geral da União, a Diretoria de Gestão de Tecnologia da Informação, responsável por disponibilizar ferramentas tecnológicas que garantam a conformidade dos processos com a Lei Geral de Dados Pessoais e com outras legislações que prevêm a restrição de dados, documentos ou processos;
- É competente para elaborar respostas para atender solicitações de acesso a informação o chefe do setor que tenha a guarda de documento ou processo institucional sem ou com restrição de acesso, sem prejuízo da necessidade de promover o tratamento dos documentos através do processo de anonimização relativa aos dados pessoais existentes e da necessidade de manter com restrição acesso as informações protegidas por sigilo legal.

3.3.2. Do Protocolo quanto à divulgação de dados não sensíveis em processos de apuração de responsabilidade ou com alteração de níveis de acesso de processos em geral:

O objetivo desse protocolo é apresentar uma opção a título de orientação ao tratamento dos riscos apresentados nas seções 3.1. e 3.2., assim como promover o atendimento ao disposto na Nota n. 00075/2024/PF-IFRN/PFIFRIO GRANDE DO NORTE/PGF/AGU, acolhida pelo Senhor Reitor do IFRN.

O presente protocolo foi construído a partir da análise e avaliação dos riscos já informados neste processo.

Protocolo quanto compartilhamento de dados não sensíveis em processos de apuração de responsabilidade ou com alteração de níveis de acesso de processos em geral

i. Objeto

- a) proteção de dados pessoais em processos com restrição de acesso.
- b) divulgação de partes não sigilosas de processos com restrição de acesso.

ii. Tratamento dos riscos envolvidos:

a) identificação:

- R1. Vazamento de dados pessoais de denunciantes, vítimas, informantes, acusado, testemunhas, e de outros envolvidos ou citados em processos correccionais.
- R2. Vazamento de dados pessoais de processos com restrição de acesso em geral;
- R3. Comprometimento do direito fundamental de acesso à informação do cidadão;
- R4. Comprometimento dos níveis de transparência ativa e passiva da instituição;
- R5. Ateste de não conformidade com a Lei de acesso à informação em processos de auditoria;
- R6. Comprometimento da imagem institucional perante os cidadãos e perante a comunidade acadêmica.

b) análise e avaliação dos riscos utilizada é a mesma metodologia empregada nos processos do IFRN que envolvem riscos de integridade, contemplando graus 1, 2, 5, 8 e 10 para probabilidade e para impacto.

Considerando que os riscos têm causas prováveis e consequências semelhantes, eles foram analisados e avaliados em um lote único, desconsiderando aspectos de causas e consequências específicas de cada risco que possa ter efeitos reduzidos ou insignificantes ao processo de gerenciamento de riscos.

Causas prováveis:

- Inexistência de um protocolo quanto ao tratamento de processos restritos em razão da existência de dados pessoais em documentos presentes no mesmo;
- Desconhecimento do fluxo de denúncias da ouvidoria por parte dos servidores do IFRN;
- Formação de servidores insuficiente para lidar com o tratamento de dados pessoais e com o acesso à informação;
- Desconhecimento dos servidores quanto à Política de Privacidade e Proteção de Dados;
- Ausência de avisos de privacidade relacionados ao tratamento de dados pessoais no âmbito do SUAP;
- Inexistência de uma política de transparência e acesso à informação institucional;
- Ausência de uma política de classificação de documentos sigilosos no âmbito do IFRN;
- Ausência de um setor de arquivo geral no IFRN e de profissionais para promover o gerenciamento institucional da guarda de documentos físicos e digitais;
- Fragilidade do módulo de processos e documentos eletrônicos do SUAP frente às novas exigências relacionadas à proteção de dados pessoais;
- Fragilidade do processo de compartilhamento de informações entre setores, dado a quantidade de pessoas existentes em alguns setores.

Consequências:

- Probabilidade aumentada de ocorrência dos riscos relacionados neste documento;
- Insegurança por parte dos servidores, gerando medo, angústia e outros elementos que podem levar ao adoecimento desses quando necessitarem tratar processos sigilosos;
- Responsabilização de servidores e gestores da instituição;
- Fragilidade do processo de gestão de riscos relacionado a guarda e tratamento de informações relacionadas a documentos e processos institucionais;
- Obsolescência do SUAP frente a outras tecnologias disponíveis ao setor público federal, a exemplo do SEI, podendo advir outras consequências desse risco.

PROBABILIDADE X IMPACTO: 8 X 8 = 64

Justifica-se a avaliação, justifica-se o nível elevado quanto à probabilidade, tendo em vista, em relação à proteção de dados, que alguns controles já foram instituídos no SUAP em relação à possibilidade de restringir o acesso aos processos para que apenas setores responsáveis e pessoas interessadas tenham acesso ao processo e documentos eletrônicos, e considerando-se, ainda as fragilidades apontadas a partir das causas prováveis. No que diz respeito aos riscos relacionados a não garantia do direito à transparência e ao acesso à informação, a probabilidade tem o nível mais alto. Assim, estando os riscos relacionados a garantia dos dois direitos fundamentais, encontrou-se o valor 8 como sendo o adequado a ser atribuído para o nível de probabilidade de ocorrência dos riscos.

Em relação ao impacto, justifica-se o grau elevado em razão de se tratar de um processo crítico que envolve a fragilidade institucional em promover a garantia de direitos individuais dos cidadãos relacionado a sua privacidade, assim como a responsabilização de gestores e servidores da instituição, assim como a imagem institucional.

Considerando a matriz de risco constante do Plano de Integridade considera como riscos aceitáveis e passíveis apenas de acompanhamento aqueles que são classificados como baixos e médios, com valores de 1 a 25, e que o valor atribuído de 64, é considerado um risco bem alto para os processos institucionais do IFRN relacionados, tem-se a necessidade e instituir um plano de tratamento considerando todas as causas prováveis, a fim de evitar a ocorrência dos riscos aqui

identificados.

c) Tratamento de riscos:

Como orientação ao tratamento de riscos, sugere-se as ações listadas a seguir para que haja o efetivo tratamento dos riscos elencados neste documento. Caso não sejam todas implementadas, sugere-se uma nova avaliação de riscos após a implementação daquelas que foram possíveis.

Id.	Ação necessária	Responsabilidade	Prazo para implementação (início com a aprovação deste plano de tratamento de riscos)
1.	Capacitar servidores para lidar com o tratamento de dados pessoais, com o acesso à informação e com a transparência de processos correcionais já concluídos e de outros processos que tenham sido classificados como restritos;	UGI (planejamento e execução)	12 meses, início imediato após planejamento
2.	Aprovação e divulgação de um protocolo quanto ao tratamento de processos restritos em razão da existência de dados pessoais em documentos presentes no mesmo;	CIGI/Reitor (aprovação); UGI (divulgação)	6 meses, início imediato, após aprovação do CGD
3.	Promover a divulgação do fluxograma de denúncias da ouvidoria junto à comunidade do IFRN, assim como normativos e atribuições relacionadas aos processos de ouvidoria;	Ouvidoria	12 meses, início imediato após planejamento
4.	Elaboração e divulgação de avisos de privacidade relacionados aos sistemas e processos que envolvem tratamento de dados pessoais;	UGI (elaboração), ASCE e DIGTI (implementação)	2 meses, início imediato
5.	Elaboração, aprovação e divulgação de uma política de transparência e acesso à informação institucional;	Comissão permanente de transparência (elaboração); CIGI (aprovação); ASCE (divulgação)	6 meses, início imediato
6.	Elaboração, aprovação e divulgação de política de classificação de documentos restritos e/ou sigilosos no âmbito do IFRN;	Reitoria (designar comissão); Comissão (elaborar política); CIGI (aprovação); Comissão (divulgar)	6 meses, início imediato
7.	Criação do setor ou atribuição competência a setor do IFRN para responsabilizar-se pelo gerenciamento institucional e guarda de documentos físicos e digitais e contratar ou capacitar servidores para atuar nesse setor;	Reitoria	ASD
8.	Atualização do módulo de processos e documentos eletrônicos do SUAP para fazer frente às novas exigências relacionadas à proteção de dados pessoais;	UGI (planejamento conjunto); DIGTI (planejamento conjunto e implementação)	4 meses, início imediato
9.	Promover adequação do processo de acesso a documentos que contenham dados sigilosos no SUAP de maneira que um aviso de privacidade surja a tela do usuário com a obrigatoriedade da ciência e concordância dos termos existentes no mesmo, caso o mesmo considere continuar com a abertura do processo e/ou documentos restritos ou sigilosos;	UGI (planejamento conjunto); DIGTI (planejamento conjunto e implementação)	4 meses, início imediato
10.	Instituição de um setor para responder como unidade setorial do Sistema de Correição do Governo Federal para que esse setor possa promover à revisão e reclassificação de processos correcionais concluídos como públicos, sem prejuízo da necessidade de promover o tratamento de dados pessoais com finalidade de anonimizar os documentos nele existentes, garantindo que informações protegidas por sigilo legal continuem restritas;	Reitoria	ASD

11.	Atribuição a uma ou a mais estruturas, setor ou formação de uma Comissão Permanente de Avaliação de Documentos Sigilosos- CPADs (Art. 34, LAI), a competência de deliberar acerca das solicitações de reclassificação de documentos hoje tidos como restritos ou sigilosos para o público, em relação a processos em geral;	Reitoria	ASD
12.	Implementação de ferramentas tecnológicas capazes de facilitar o processamento da anonimização de dados pessoais em documentos e processos eletrônicos;	UGI (planejamento conjunto e capacitação); DIGTI (planejamento conjunto e implementação)	12 meses, início imediato
13.	Fortalecimento das estruturas funcionais que tratam da proteção de dados pessoais, transparência e segurança da informação para atuar nesse processo de formação dos servidores, promover orientações, formular políticas internas que tratem da classificação de processos e documentos.	Reitoria	ASD
14.	Promoção de formação de pelo menos dois servidores por setor sistêmico e por campus acerca do processo de tratamento de documentos ou processos com restrição de acesso, sendo esses servidores credenciados a tramitar processos restritos no âmbito dos setores.	UGI (capacitação); DIGTI (melhoria do SUAP e credenciamento dos servidores)	4 meses
15.	Promoção de melhoria no SUAP, com a criação de um perfil para que os servidores que receberam o treinamento para tramitar esses processos, possa fazê-lo com a segurança necessária;	DIGTI (melhoria do SUAP e credenciamento dos servidores)	4 meses
16.	Promoção de melhoria no SUAP, com o objetivo de só considerar público documentos que efetivamente tenham sido compartilhados. Documentos que não foram compartilhados devem permanecer automaticamente na condição de documento restrito ao operador que o elaborou;	CGD (aprovar a proposta de melhoria); DIGTI (se aprovado, implementar melhoria no SUAP)	4 meses
17.	Promover melhoria no SUAP para que somente a autoridade competente possa classificar um documento como sigiloso, com grau de restrição classificado como sendo de natureza ultrassecreta, secreta ou reservada, nos termos da Lei.	DIGTI (melhoria do SUAP e credenciamento dos servidores)	4 meses

iii. Do protocolo para compartilhamento de processos correcionais.

O presente protocolo foi criado a partir de orientações da CGU constantes na Nota Técnica nº 2418/2023/CGUNE/DICOR/CRG, da Lei Geral de Dados Pessoais e da Lei de Acesso à Informação. Este se aplica a todos os processos correcionais, sendo a base legal para as ações e providências propostas por este protocolo.

Ação/protocolo	Responsável	Tratamento de dados pessoais	Providências necessárias	Finalidade
O julgamento de processos administrativos disciplinares deve ser publicado no Boletim de serviço do IFRN, desde que não se trate de PADs nos quais se apliquem sanções expulsivas, cujas decisões de julgamento, por simetria ao disposto no art. 1º, inciso I, da Lei nº 4.965, de 1966, deverão ser publicadas no DOU.	Gabinete/Secretaria do Gabinete	Publicação	Revisão do fluxo atual	Transparência ativa

O nome do servidor apenado e sua matrícula SIAPE enquadram-se como informações de interesse coletivo ou geral, razão pela qual não se justifica a ocultação dessas duas informações quando da publicidade do resultado do PAD que resultou em sanção disciplinar.	Gabinete/Secretaria do Gabinete	Publicação	Revisão do fluxo atual	Transparência ativa
Quando decidido pelo arquivamento de PADs ordinários, a decisão deverá ser publicada sem menção ao nome do servidor processado nem à sua matrícula, citando-se apenas o número do PAD e os seis números do meio do CPF.	Gabinete/Secretaria do Gabinete	Publicação com anonimização de dados pessoais	Revisão do fluxo atual; treinamento quanto ao processo de anonimização dos dados pessoais	Transparência ativa; proteção de dados pessoais
Os processos administrativos disciplinares são de acesso restrito enquanto estiverem em curso, mas, uma vez julgados, passam a ser públicos, sem prejuízo da proteção das informações pessoais e legalmente sigilosas, as quais deverão ser mantidas com restrição de acesso.	Gabinete/Secretaria do Gabinete	Alteração de status, revisão e anonimização de dados pessoais em documentos do processo	Revisão do fluxo atual; treinamento quanto ao processo de anonimização dos dados pessoais	Transparência ativa; proteção de dados pessoais
A mudança de status do processo administrativo disciplinar, de sigiloso/restrito para público, ocorre integral e automaticamente, a partir do respectivo julgamento, semelhante ao que ocorre no disposto no Enunciado CGU nº 6/2023 – Abertura de informações desclassificadas, devendo o processo passar por uma revisão do setor responsável para garantir que documentos que contenham dados pessoais continuem com a restrição legal prevista.	Gabinete/Secretaria do Gabinete	Alteração de status, revisão e anonimização de dados pessoais	Revisão do fluxo atual; treinamento quanto ao processo de anonimização dos dados pessoais	Transparência ativa; proteção de dados pessoais
A mudança de status da publicidade do processo disciplinar, mencionada no item anterior, ocorre a partir de seu julgamento, independentemente de encontrar-se pendente o julgamento de recurso ou o transcurso de prazo recursal.	Gabinete/Secretaria do Gabinete	Alteração de status, revisão e anonimização de dados pessoais	Revisão do fluxo atual; treinamento quanto ao processo de anonimização dos dados pessoais	Transparência ativa; proteção de dados pessoais
A íntegra do PAD não é considerada informação de interesse coletivo ou geral nos termos do art. 7º do Decreto nº 7.724, de 16 de maio de 2012, razão pela qual não se exige a disponibilização dos processos em transparência ativa.	Chefe do setor designado formalmente para exercer a competência de órgão setorial do SISCOR	Restrição ao público externo	Designação de setor responsável por exercer a competência de órgão setorial do SISCOR	Transparência passiva; proteção de dados pessoais

Quando solicitado o acesso ao processo concluído, o órgão deve promover a disponibilização de cópia, suprimidas as informações protegidas por sigilo legal e as informações pessoais, através do processo de anonimização de dados pessoais. Documentos em que a anonimização das informações não for possível, esses deverão permanecer restritos e não devem ser disponibilizados.	Chefe do setor designado formalmente para exercer a competência de órgão setorial do SISCOR.	Disponibilização, revisão e anonimização de dados pessoais	Treinamento quanto ao processo de anonimização dos dados pessoais; designação de setor responsável por exercer a competência de órgão setorial do SISCOR; elaboração de rotina junto às comissões de PAD para um melhor tratamento dos dados pessoais, facilitando o processo de anonimização dos dados pessoais.	Transparência passiva; proteção de dados pessoais
É razoável a prática de realizar a disponibilização do PAD encerrado por meio de versão resumida contendo seus principais documentos, dado que se encontra em conformidade com as diretrizes dos §§ 2º e 3º do art. 7º da LAI, na seção da Corregedoria da página de acesso à informação.	Chefe do setor designado formalmente para exercer a competência de órgão setorial do SISCOR.	Publicação, revisão e anonimização de dados pessoais	Treinamento quanto ao processo de anonimização dos dados pessoais; designação de setor responsável por exercer a competência de órgão setorial do SISCOR; elaboração de rotina junto às comissões de PAD para um melhor tratamento dos dados pessoais, facilitando o processo de anonimização dos dados pessoais.	Transparência ativa; proteção de dados pessoais

A versão resumida do PAD deverá conter, ao menos, a portaria de instauração do processo, o termo de indicição, o relatório final da comissão processante, os pareceres apresentados no processo que servirem de base para o julgamento, a decisão de julgamento e a decisão em sede de recurso ou pedido de reconsideração, se houver, promovendo o tratamento das informações protegidas por sigilo legal e as informações pessoais.	Chefe do setor designado formalmente para exercer a competência de órgão setorial do SISCOR	Revisão e anonimização de dados pessoais	Treinamento quanto ao processo de anonimização dos dados pessoais; designação de setor responsável por exercer a competência de órgão setorial do SISCOR; elaboração de rotina junto às comissões de PAD para um melhor tratamento dos dados pessoais, facilitando o processo de anonimização dos dados pessoais.	Transparência ativa; proteção de dados pessoais
A disponibilização da versão resumida do PAD não exclui o direito do cidadão de obtenção da íntegra desse processo, devendo-se, na resposta do pedido de acesso à informação, comunicar ao requerente a possibilidade de ser solicitado expressamente acesso à íntegra dos autos, devendo-se proceder ao tratamento das informações protegidas por sigilo legal e as informações pessoais para a posterior disponibilização.	Chefe do setor designado formalmente para exercer a competência de órgão setorial do SISCOR	Disponibilização, revisão e anonimização de dados pessoais	Treinamento quanto ao processo de anonimização dos dados pessoais; designação de setor responsável por exercer a competência de órgão setorial do SISCOR; elaboração de rotina junto às comissões de PAD para um melhor tratamento dos dados pessoais, facilitando o processo de anonimização dos dados pessoais.	Transparência passiva; proteção de dados pessoais

iv. Do protocolo para compartilhamento de processos com restrição de sigilo em face da existência de dados pessoais ou dados pessoais sensíveis.

O presente protocolo foi elaborado com a finalidade de atender o Artigo 7º da Lei de Acesso à Informação e considerando o princípio da finalidade estabelecido na Lei Geral de Proteção de Dados Pessoais, além de outros dispositivos legais informados no texto.

Ação/protocolo	Responsável	Tratamento de dados pessoais	Providências necessárias	Finalidade
Disponibilização por meio de transparência passiva de documentos e/ou processos que guardem algum tipo de sigilo legal ou informações pessoais.	Setores responsáveis pelo arquivamento dos documentos e/ou processos em meio digital e, em meio físico, se ainda estiver localizado no respectivo setor. Existindo arquivo no Campus ou Reitoria para a guarda de processos e/ou documentos em meio físico, o responsável pela disponibilização é o chefe do setor de arquivos, devendo esse consultar a área responsável pela informação antes de disponibilizar o documento e/ou processo.	Disponibilização mediante solicitação em transparência passiva	Promover a disponibilização dos documentos e/ou processos, se for possível promover a anonimização das informações sigilosas e informações pessoais; treinamento quanto ao processo de anonimização dos dados; criar setor ou atribuir competência a setor e/ou comissão permanente responsável pela revisão e guarda de documentos e pela elaboração e implementação de uma política de classificação de documentos.	Transparência passiva
Processos e documentos que haja possibilidade de passar por um processo de anonimização dos dados pessoais presentes e que tenham sido classificados como restritos ou sigilosos por esse único motivo, devem ser reclassificados como públicos e disponibilizados para consulta em transparência ativa por meio de processo de pesquisa simples em módulo já existente de documentos e/ou processos eletrônicos.	DIGTI, com respaldo do setor e/ou comissão permanente responsável pela revisão e guarda de documentos e pela elaboração e implementação de uma política de classificação de documentos.	Disponibilização por meio de consulta eletrônica em transparência ativa	Reclassificar processos tidos como restritos em públicos; anonimização dos documentos presentes no processo; treinamento quanto ao processo de anonimização dos dados pessoais; criar setor ou atribuir competência a setor e/ou comissão permanente responsável pela revisão e guarda de documentos e pela elaboração e implementação de uma política de classificação de documentos.	Transparência ativa

A íntegra de um processo protegido por sigilo legal não é considerada informação de interesse coletivo ou geral nos termos do art. 7º do Decreto nº 7.724, de 16 de maio de 2012, razão pela qual não se exige a disponibilização dos processos em transparência ativa.	Setores responsáveis pelo arquivamento dos documentos e/ou processos em meio digital e, em meio físico, se ainda estiver localizado no respectivo setor. Existindo arquivo no Campus ou Reitoria para a guarda de processos e/ou documentos em meio físico, o responsável pela disponibilização é o chefe do setor de arquivos, devendo esse consultar a área responsável pela informação antes de disponibilizar o documento e/ou processo.	Restrição ao público externo	Criar setor ou atribuir competência a setor e/ou comissão permanente responsável pela revisão e guarda de documentos e pela elaboração e implementação de uma política de classificação de documentos.	Transparência passiva; proteção de dados pessoais
---	--	------------------------------	--	---

v. Do processo de anonimização de dados pessoais.

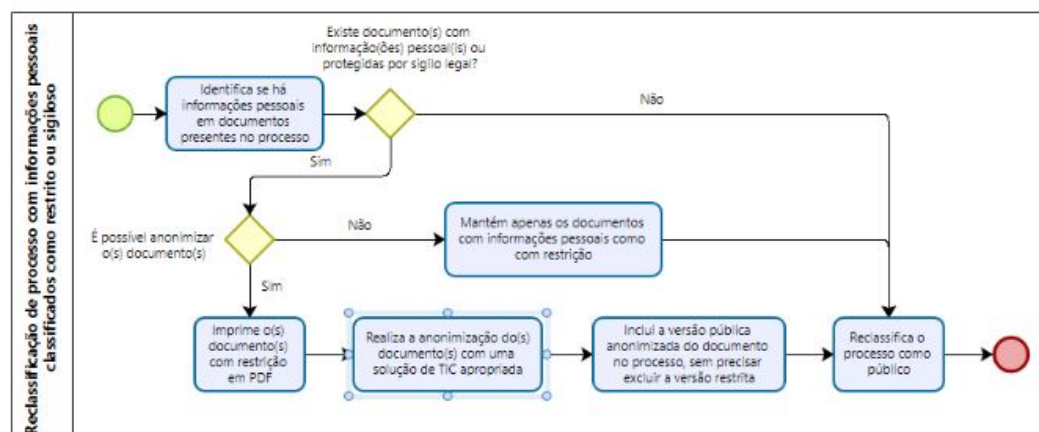
A LGPD considera "dado anonimizado", como "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

Assim, o processo de anonimização dos dados pessoais proposto, enquanto a Diretoria de Gestão de Tecnologia da Informação não disponibiliza uma ferramenta própria do IFRN para essa finalidade, é o processo manual realizado por meio do software Foxit Reader, em sua versão gratuita, com o uso de ferramentas de destaque de texto ou de área em cor preta e fazendo uso do mecanismo de impressão de figura em PDF não editável.

Ressaltamos que o processo descrito foi devidamente testado pela área de segurança da informação do IFRN e que se trata de um processo de anonimização irreversível.

Na figura a seguir, apresenta-se um fluxo do processo de anonimização de dados pessoais, considerando um processo que tenha sido considerado restrito ou sigiloso em função de um ou mais de seus documentos conter(em) informação(ões) pessoal(is):

Figura 1: Fluxograma de reclassificação de processo com restrição informada em razão da existência ou inexistência de dados pessoais, de restrito (ou sigiloso) para público.



Fonte: elaboração própria.

Documento assinado eletronicamente por:

- **Ismael Felix Coutinho Neto**, **Chefe da Unidade de Gestão da Integridade - FAG-IFRN - UGI**, em 15/10/2024 16:00:42.

Este documento foi emitido pelo SUAP em 27/09/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifrn.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 774113

Código de Autenticação: 2a7fd299d3

