TRIBUNAL DE CONTAS DA UNIÃO

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

(RIPD)

NO ÂMBITO DAS CONTRATAÇÕES DO TCU

REPÚBLICA FEDERATIVA DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

TCU

TRIBUNAL DE CONTAS DA UNIÃO

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

(RIPD)

NO ÂMBITO DAS CONTRATAÇÕES DO TCU

Brasília, 2021

SUMÁRIO

APRESENTAÇÃO 7

1. PRESSUPOSTOS TEÓRICOS E METODOLÓGICOS 11

2. CONTEÚDO 19
2.1. DESCRIÇÃO DO PROCESSO DE TRATAMENTO 19

2.1.1. FASE DE LICITAÇÃO 20

2.1.2. FASE DE EXECUÇÃO CONTRATUAL 21

2.2. DESCRIÇÃO DOS TIPOS DE DADOS PESSOAIS COLETADOS E ..... DO MÉTODO DE COLETA DE DADOS 24

2.3. RISCOS NA PROTEÇÃO DE DADOS 25

2.4. MEDIDAS DE SALVAGUARDA E MITIGAÇÃO DE RISCOS 26

2.4.1. CLASSIFICAÇÃO DA INFORMAÇÃO 29

2.4.2. DESCARTE DE DADOS PESSOAIS PELOS FISCAIS DE CONTRATOS E PELA COMISSÃO DE LICITAÇÃO OU PELO PREGOEIRO 30

2.4.3. REVISÃO DAS REGRAS DE ACESSO AO SISTEMA ÁUREA E A SUAS FUNCIONALIDADES 31

2.4.4 FIXAÇÃO DE CRITÉRIOS DE TEMPORALIDADE PARA GUARDA DE DOCUMENTOS ELETRÔNICOS DE FISCALIZAÇÃO DE CONTRATOS NO SISTEMA E-TCU 32

2.4.5. EXPEDIÇÃO FORMAL DE ORIENTAÇÃO PARA AGENTES QUE ATUAM NOS PROCESSOS DE CONTRATAÇÃO E GESTÃO CONTRATUAL 33

2.4.6. PADRONIZAÇÃO DE CLÁUSULAS CONTRATUAIS QUE ESTABELEÇAM A OBRIGAÇÃO DE AS EMPRESAS TERCEIRIZADAS ENVIAREM OS DADOS PESSOAIS AO TCU DE FORMA CRIPTOGRAFADA E CONTENDO EXCLUSIVAMENTE OS DADOS DE FUNCIONÁRIOS EM EXERCÍCIO NO TCU 34

2.5. AVALIAÇÃO DAS MEDIDAS DE MITIGAÇÃO DE RISCOS 34

2.5.1. CLASSIFICAÇÃO DA INFORMAÇÃO 35

2.5.2. DESCARTE DE DADOS PESSOAIS PELOS FISCAIS DE CONTRATOS E PELA COMISSÃO DE LICITAÇÃO OU PELO PREGOEIRO 36

2.5.3. REVISÃO DAS REGRAS DE ACESSO AO SISTEMA ÁUREA E A SUAS FUNCIONALIDADES 37

2.5.4. FIXAÇÃO DE CRITÉRIOS DE TEMPORALIDADE PARA GUARDA DE DOCUMENTOS DE FISCALIZAÇÃO DE CONTRATOS NO SISTEMA E-TCU 38

2.5.5. EXPEDIÇÃO FORMAL DE ORIENTAÇÃO PARA AGENTES QUE ATUAM NOS PROCESSOS DE CONTRATAÇÃO E GESTÃO CONTRATUAL 38

2.5.6. PADRONIZAÇÃO DE CLÁUSULAS CONTRATUAIS QUE ESTABELECEM A OBRIGAÇÃO DE AS EMPRESAS TERCEIRIZADAS ENVIAREM OS DADOS PESSOAIS AO TCU DE FORMA CRIPTOGRAFADA E CONTENDO EXCLUSIVAMENTE OS DADOS DE FUNCIONÁRIOS EM EXERCÍCIO NO TCU 39

3. CONCLUSÕES E ENCAMINHAMENTO 41

APRESENTAÇÃO

A Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) implementou relevantes e inovadoras alterações na sistemática de proteção de dados pessoais no Brasil, tratados tanto por meio físico quanto digital. O objetivo da norma, enunciado em seu art. 1°, é "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Com efeito, na sociedade contemporânea, os dados pessoais assumem importância estratégica. Constituem valiosos ativos para negócios de inúmeras espécies. E, com o desenvolvimento das tecnologias de comunicação e compartilhamento de informações, não raro são utilizados em situações de risco a liberdades e garantias fundamentais. Os cidadãos, nesse novo cenário, sujeitam-se a vulnerabilidades na autonomia informativa sobre seus próprios dados.

A LGPD veio, então, congregar um sistema normativo direcionado a evitar riscos relacionados ao tratamento de dados e informações, por instituições públicas e privadas, de modo a proporcionar segurança e transparência aos titulares de dados. A norma permite o controle dos dados pelos interessados, impõe deveres e responsabilidades aos agentes de tratamento e proporciona segurança à circulação de informações. Em síntese, a LGPD inspira e impõe um tratamento mais ético e seguro dos dados pessoais.

No entanto, não se pode negar que se trata de um marco regulatório complexo. A LGPD tem sido amplamente debatida em muitos fóruns, mormente com ênfase em aspectos conceituais e jurídicos. Pouco ainda há de consenso sobre o que se pode fazer para atender a lei. De todo

modo, sabe-se que a edição da norma é um passo decisivo na formação de uma cultura de proteção de dados pessoais no país.

Há, portanto, muitos desafios a vencer na construção de modelos seguros de tratamento de dados pessoais, alinhados à nova LGPD. No âmbito da Administração Pública, especificamente, soma-se a esses desafios o grande volume de dados pessoais geridos em numerosas e pulverizadas atividades. Ademais, há o interesse público, que, como um fim necessário de toda a atuação administrativa, perpassa as discussões sobre o tratamento de dados pessoais, associando-se a outros princípios, como o da transparência.

Para tratar dessas nuances, a LGPD reservou capítulo específico para a Administração Pública. Pelo que se extrai das disposições legais, dada a relação assimétrica estabelecida entre o poder público e os titulares de dados, é dever dos órgãos e das entidades da Administração Pública potencializar a segurança e transparência. A "transparência visa a inspirar no titular de dados a credibilidade no ente público controlador dos dados e a necessária responsabilidade a que está submetido, numa clara relação com um princípio peculiar da lei protetiva nacional, o da responsabilização e prestação de contas."[1]

Enfim, ainda com mais veemência na Administração Pública, é necessário e urgente caminhar para a consolidação de práticas de governança em segurança e privacidade de dados capazes de fornecer aparato institucional que dê substância à infraestrutura legal consolidada pelo novo marco.

É nesse contexto, no esforço para agregar aos sistemas de gestão do Tribunal de Contas da União (TCU) tais instrumentos de governança, que se apresenta o presente **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**.

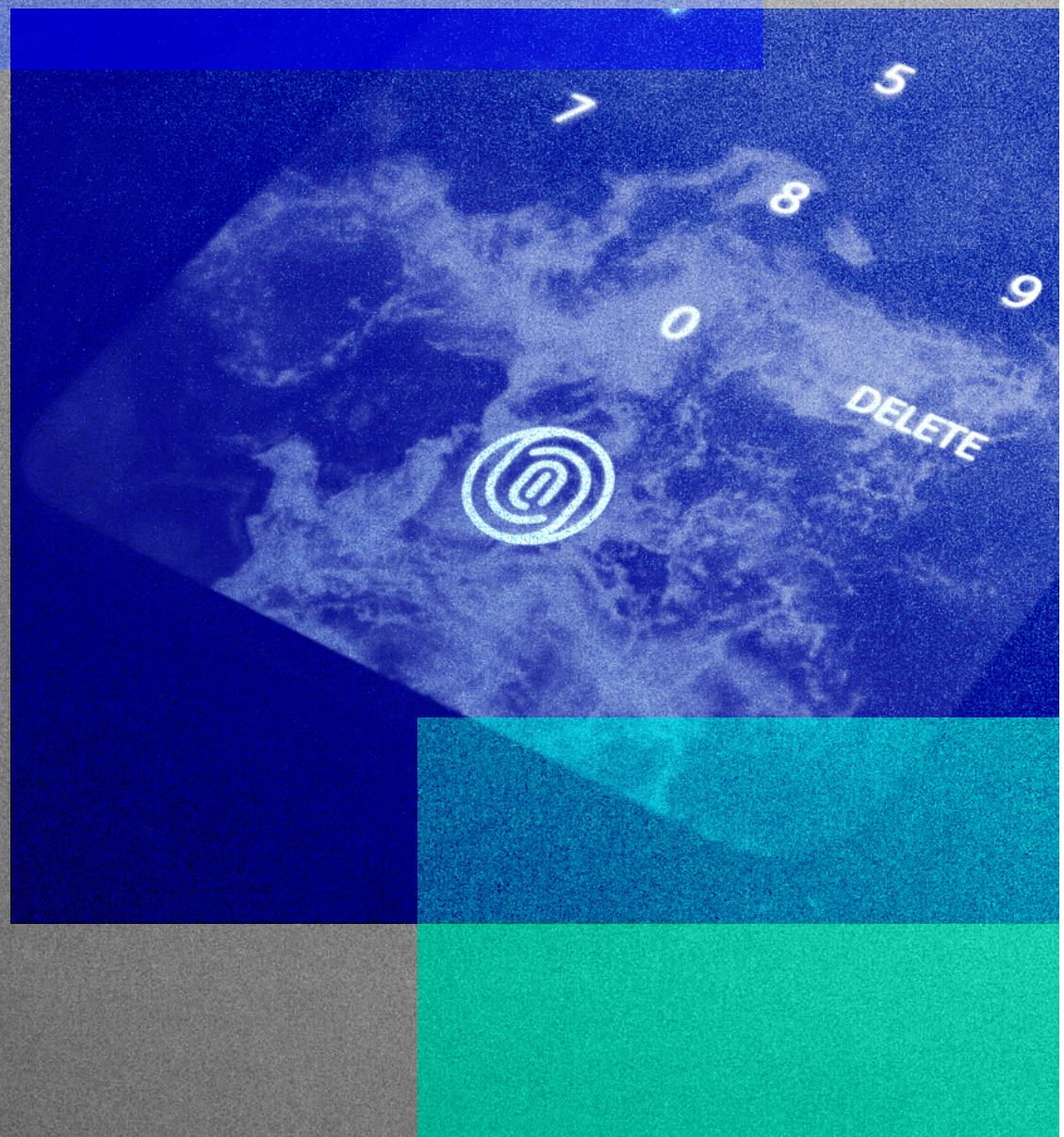
Cabe ressaltar que este relatório diz respeito somente às **atividades e aos processos de trabalho da área administrativa de contratações do Tribunal**. Dada a variedade de ações desenvolvidas pelo TCU, tanto na área meio quanto finalística, às quais são associadas peculiaridades bastante distintas, e tendo em vista, ainda, a natureza pioneira do trabalho, optou-se por desenvolvê-lo exclusivamente nos limites das atividades afetas a contratações de bens e serviços realizadas pela Secretaria de Licitações, Contratos e Patrimônio (Selip). Trata-se do primeiro documento da espécie elaborado no âmbito do TCU. O aprendizado e a experiência adquirida certamente servirão de base para outros RIPDs.

O enfoque do relatório nos dados tratados em processos de trabalho próprios de contratações e gestão contratual é fruto da cooperação entre a Selip e Secretaria de Ouvidoria e Segurança da Informação (Sesouv). A Sesouv, atuando em função das competências previstas no inc. XIX do art. 25 da Resolução TCU 324/2020, coordenou as atividades que resultaram na produção deste RIPD. Por sua vez, a Secretaria-Geral Adjunta de Administração (Adgedam) acompanhou o trabalho e colaborou em todas as etapas, prestando auxílio e supervisão.

Considerou-se, para a seleção do escopo, além da vontade manifestada pela Selip de atuar com mais rigor na proteção de dados pessoais e do empenho das equipes da unidade nesse sentido, a natureza das atividades em foco. É inerente às atividades de contratação e gestão contratual o manejo de uma grande quantidade de dados pessoais, sobretudo de representantes legais e prestadores de serviços, alguns potencialmente sensíveis. O tratamento desses dados se mostra, por isso, ponto nevrálgico para uma boa governança em segurança e privacidade. Ademais, têm sido recorrentes dificuldades interpretativas, relacionadas a uma aparente colisão entre a proteção de dados pessoais e o acesso à informação – outra base principiológica a ser seguida nas contratações públicas.

A escolha do escopo revelou-se, ao fim, realmente propícia. O produto alcançado, materializado neste relatório, mostra-se rico e efetivo na antecipação e no tratamento de riscos à proteção de dados pessoais, observados os mandamentos da transparência. É um bom começo no caminho para a consolidação da governança em segurança e proteção de dados nas contratações do TCU. Essa jornada, para além do esforço e custo empreendidos, por certo, representa uma valiosa janela de oportunidade e inovação.

[1] TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo poder público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Org.). **LGPD**: Lei Geral de Proteção de Dados comentada (livro eletrônico). 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020.



1. PRESSUPOSTOS TEÓRICOS E METODOLÓGICOS

Conforme a definição contida no art. 5°, inciso XVI, da LGPD, o Relatório de Impacto à Proteção de Dados é a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

Com base nas disposições da lei, foram os seguintes os requisitos considerados essenciais para a elaboração deste RIPD:

ITEM	REQUISITO	FUNDAMENTO
1	Descrição do processo de tratamento	Art. 5º, XVII, da LGPD
2	Descrição dos tipos de dados pessoais coletados	Parágrafo único do art. 38 da LGPD
3	Método de coleta dos dados pessoais	Parágrafo único do art. 38 da LGPD
4	Riscos na proteção de dados pessoais	Não há fundamento legal direto, mas este requisito é mero corolário da necessidade de indicar medidas de mitigação de riscos (não é possível indicar medidas de mitigação dos riscos sem a identificação de tais riscos)
5	Medidas de salvaguarda e mitigação de riscos e metodologia para garantir a segurança das informações	Art. 5º, XVII, c/c o parágrafo único do art. 38 da LGPD
6	Análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados	Parágrafo único do art. 38 da LGPD

As descrições suscintas dos processos de tratamento e dos tipos de dados coletados – primeiras etapas – foram realizadas pelas equipes da Selip, mediante o preenchimento de planilhas de dados e informações especialmente elaboradas para esse fim, sob a supervisão da Sesouv.

Reunidos esses elementos essenciais, foi realizada uma oficina, no dia 23/9/2021, sob a coordenação da Sesouv, da qual participaram servidores da Selip com conhecimento e experiência nos processos de trabalho. O objetivo foi o refinamento e tratamento das informações já colhidas e desenvolvimento das demais etapas para elaboração do RIPD, quais sejam: descrição dos processos de trabalho, especificação da forma de coleta dos dados, identificação de riscos na proteção de dados, bem como análise e avaliação de informações.

Para contexto, identificação, análise e avaliação dos riscos foram seguidas as etapas da ISO 31.000/2018.[2]

Como a LGPD expressamente estabelece que os riscos devem ser mitigados (art. 5º, XVII, e parágrafo único do art. 38), foi adotado o conceito de risco pelo viés negativo, segundo o qual o risco é um evento que pode afetar adversamente o alcance dos objetivos relacionados à proteção de dados pessoais.

Segundo a ISO 31.000, "escopo, contexto e critérios envolvem a definição do escopo do processo, a compreensão dos contextos externo e interno". Faz parte da fase, também, a definição da forma de mensuração da probabilidade e do impacto dos riscos.

Tanto na probabilidade quanto no impacto foi utilizada a sequência de Fibonacci (3, 5, 8, 13 e 21), considerando as vantagens apontadas por Benedito Antônio da Costa[3].

A escala utilizada para probabilidade foi a relacionada a seguir.

Quadro 1 –Critérios de probabilidade

	PROBABILIDADE	CRITÉRIOS
3	Muito Baixo	Acontece em situações excepcionais. Não há histórico conhecido do evento e/ou não há indícios que sinalizem sua ocorrência.
5	Baixo	Ocorrência casual. Há histórico conhecido do evento e/ou há poucos indícios de que possa acontecer no futuro.
8	Médio	Repete-se ao longo dos anos com frequência reduzida e/ou há indícios de que possa ocorrer no futuro.
1 3	Alto	Repete-se todos os anos, poucas vezes ao ano e/ou há muitos indícios de que vá ocorrer em futuro próximo.
2 1	Muito Alto	Repete-se todos os anos, muitas vezes ao ano e/ou é praticamente certo que ocorrerá em futuro próximo.

Fonte: Elaborado pela Sesouv.

[3]Associação Brasileiras de Normas Técnicas, **NBR ISO 31.000**: Gestão de Riscos: Diretrizes. Rio de Janeiro: 2018.
[2]BRASIL. Tribunal Regional Eleitoral de Mato Grosso. **Revista Democrátic**a. Costa, Benedito Antônio. Utilização da Escala de Fibonacci na avaliação de riscos: vantagens, aplicações e didática. Volume 5. Cuiabá: 2019.

Quadro 2 – Critérios de impacto

	IMPACTO	CRITÉRIOS
3	Muito Baixo	(a) Efeito na imagem da contratação (b) Não observância de boas práticas em proteção de dados
5	Baixo	(a) Efeito na imagem da equipe envolvida com a contratação (b) Descumprimento de norma interna (resolução, portaria) de proteção de dados
8	Médio	(a) Efeito na Imagem Selip (b) Descumprimento de decretos, de instruções normativas ou de determinações de acórdãos em proteção de dados
13	Alto	(a) Efeito reversível na imagem do TCU (b) Desconformidade legal (ex: Lei 14.133, LGPD, LAI)
21	Muito Alto	(a) Efeito de difícil reversão na imagem do TCU (b) Descumprimento mandato legal finalístico (constitucional, legal, etc)

Fonte: Elaborado pela Sesouv.

Também foi definido que o nível de risco será determinado pela multiplicação da nota do fator de probabilidade pela nota do fator de impacto, podendo ser obtidas as seguintes combinações, expressas no mapa de calor abaixo.

Figura 1 – Níveis de risco

	NÍVEIS DE RISCO					
PROBABILIDADES	21	63	105	168	273	441
	13	39	65	104	169	273
	8	24	40	64	104	168
	5	15	25	40	65	105
	3	9	15	24	39	63
		3	**5**	**8**	**13**	**21**
		IMPACTO				

Fonte: Elaborado pela Sesouv.

Assim, segundo o mapa de calor apresentado, os riscos de nível 9 são considerados “muito baixos”. Os riscos de níveis 15 a 25 são considerados “baixos”. Os riscos de níveis 40 a 65 são considerados “médios”. Os riscos de níveis 104 a 169 são considerados “altos”. Por fim, os riscos de níveis 273 a 441 são considerados “muito altos”.

Eleitos os critérios acima, foi estabelecido o contexto do processo de gestão de riscos, que deve servir ao cumprimento dos seguintes requisitos, para elaboração do RIPD: descrição do processo de tratamento, descrição dos tipos de dados coletados e método de coleta dos dados pessoais.

Para esse fim, foi preenchida a planilha Template Contexto Riscos LGPD, que contém o objeto da gestão de riscos, as etapas do processo de contratação e suas descrições, os principais setores, gestores e servidores envolvidos, os controles existentes e os principais comandos legais que devem ser atendidos.

Ressalta-se, ainda, que as expressões “dado pessoal”, “dado pessoal sensível”, “titular”, “tratamento de dados” e “controlador”, utilizadas ao longo do relatório, foram empregadas na acepção contida no art. 5° da LGPD.

2. CONTEÚDO

2.1. DESCRIÇÃO DO PROCESSO DE TRATAMENTO

Para delimitar o contexto de tratamento dos dados pessoais, em linha com a divisão dos processos de trabalho desenvolvidos na Selip, foram consideradas quatro fases do processo de contratação, quais sejam: planejamento da contratação, processo licitatório, fase de formalização da contratação e fase de execução contratual.

Em todas as fases, as bases legais para o tratamento dos dados pessoais são **o cumprimento de obrigação legal**, previsto no inciso II do art. 7° da LGPD, e **a persecução do interesse público, com objetivo de executar competências legais ou cumprir atribuições legais do serviço público**, conforme prevê o art. 23 da LGPD.

A **fase de planejamento da contratação** envolve as atividades de identificação da necessidade de contratação; elaboração de estudos técnicos preliminares; pesquisa de preços; confecção de termo de referência e edital, conforme o caso; obtenção de reserva orçamentária; emissão de parecer da Consultoria Jurídica do TCU; avaliação de conveniência e oportunidade da contratação; e, por fim, autorização para contratar.

A **fase de licitação**, correspondente à fase externa dos certames, é formada pelas atividades de publicação de aviso de licitação; recebimento de propostas e pedidos de esclarecimentos ou impugnações; realização de sessão pública; julgamento de propostas; habilitação de empresas; julgamento de recursos; e adjudicação e homologação.

A **fase de formalização da contratação** consiste na emissão do empenho que suportará a despesa com a contratação e nos procedimentos de assinatura do termo contratual, quando for o caso.

A **fase de execução contratual** é formada pela emissão de ordens de serviços; pela fiscalização (subdividida em conformidade previdenciária, fiscal e trabalhista, eventuais apurações de responsabilidade e aplicação de sanções); pelo recebimento de serviços; pelos procedimentos de pagamento; e pelas atividades de gestão contratual, quais sejam: prorrogações, alterações, repactuações e reajustes para atualização dos valores dos contratos.

Identificou-se que, das quatro fases do processo de contratação, o tratamento de dados pessoais ocorre, principalmente, nas fases de licitação e execução contratual.

2.1.1. FASE DE LICITAÇÃO

Na fase de licitação são coletados apenas dados pessoais cadastrais relativos aos representantes das empresas, como nome, CPF e RG. Esses dados são fornecidos pelos titulares, como condição para participar dos certames ou firmar contratos, inclusive no corpo de documentos de habilitação e propostas. Os dados são inseridos diretamente pelos titulares nos sistemas governamentais que operacionalizam os processos de contratação ou lhes dão suporte. No caso das contratações realizadas pelo TCU, que é órgão não integrante do Sistema de Serviços Gerais do Poder Executivo (Sisg), os principais sistemas a serem considerados são o Comprasnet e o Sistema de Cadastramento Unificado de Fornecedores (Sicaf).

As contratações são documentadas internamente, no âmbito dos processos de trabalho do TCU, em processos específicos, do tipo administrativo, autuados principalmente na própria Selip, no sistema e-TCU. Essa documentação é indispensável não só para viabilizar e organizar o fluxo do processo de trabalho, mas para permitir a adoção de controles internos e externos, inclusive auditorias. Em tais processos, são reproduzidos documentos extraídos dos sistemas governamentais já aludidos em que constam os dados pessoais fornecidos pelos titulares, como cópias de documentos pessoais, atas, relatórios e certidões.

Ademais, os mesmos dados são referenciados, nos processos, em instruções e despachos, como análises e julgamentos de recursos e impugnações, análises de propostas e instruções de propostas de sanção.

Não há, na etapa de realização do certame, qualquer espécie de tratamento de dados pessoais para fins divergentes daqueles pretendidos com o próprio processo de contratação. Em síntese, os dados são necessários para identificar os representantes legais das empresas licitantes e possibilitar o controle e a detecção de fraudes. Trata-se de dados de acesso público.

Cabe destacar que, no âmbito do tratamento no TCU, os dados não são compartilhados ou modificados.

Há, ainda, possibilidade de, na fase de licitação, serem coletados dados pessoais por outros meios que não os sistemas governamentais. É também possível que tais dados sejam manuseados e armazenados, internamente, em outros ambientes ou meios além dos processos do e-TCU. É o que ocorre, por exemplo, com os documentos enviados por e-mail.

2.1.2. FASE DE EXECUÇÃO CONTRATUAL

A fase de execução contratual foi considerada a mais crítica no que diz respeito ao tratamento de dados pessoais. A atividade de fiscalização de contratos de terceirização, mais especificamente, implica o tratamento de volume expressivo de dados pessoais, por força dos procedimentos de conformidade documental relativa a encargos trabalhistas e previdenciários das contratadas.

Como é cediço, a Administração é responsável subsidiária pelas verbas trabalhistas decorrentes da execução dos contratos que firma e responsável solidária pelos encargos previdenciários. Como decorrência necessária dessa responsabilidade, tem o dever de fiscalizar o efetivo adimplemento dos aludidos encargos pelas empresas contratadas, mediante procedimentos de análise individualizada de documentação trabalhista e previdenciária.

No TCU, tais procedimentos são regulamentados pela Portaria TCU 444/2018. Cabe destacar que, mais recentemente, a Lei 14.133/2021 – nova lei de licitações e contratos administrativos – tratou dos procedimentos de fiscalização em contratos de terceirização. A norma, já vigente, não inova significativamente na matéria. Ao contrário, estabelece rotinas, obrigações e processos de trabalho harmoniosos com a prática até então adotada pelo TCU, constante do mencionado regulamento interno.

Para cumprir as rotinas previstas na Portaria-TCU 444/2018, são tratados dos dados de prestadores de serviços alocados em contratos, constantes dos seguintes documentos: carteiras de trabalho, exames médicos admissionais e demissionais, cópias de contracheques, comprovantes de transferências bancárias, cópias de extratos do Instituto Nacional do Seguro Social (INSS) e Fundo de Garantia do Tempo de Serviço (FGTS), folhas de ponto, avisos de férias, guias de recolhimento do FGTS e informações à Previdência Social – Guia de Recolhimento do FGTS e de Informações à Previdência Social (GFIP).

Portanto, constatou-se que, de todo o processo de contratação, o tratamento de dados pessoais ocorre de maneira mais significativa durante a fase de execução contratual, na atividade de fiscalização de contratos de terceirização.

Durante a execução das atividades de fiscalização, a empresa contratada envia a documentação contendo os dados pessoais para o fiscal de contrato, normalmente via e-mail ou documento eletrônico e, em alguns casos, documento físico (ofício, comunicação etc.). Assim, a coleta dos dados é feita por intermédio da empresa contratada, que os fornece sem a participação direta dos titulares dos dados no processo.

Ao receber a documentação, o fiscal de contrato cadastra os documentos no Sistema de Gestão de Aquisições das Unidades do TCU nos Estados e Conformidade (Áurea), utilizado para verificação da conformidade previdenciária, fiscal e trabalhista das empresas contratadas, dando início, assim, à checagem de regularidade.

Os dados pessoais constantes do sistema Áurea são, ao fim do período de análise de regularidade a que se referem, convertidos em documentos eletrônicos do e-TCU. Os documentos eletrônicos podem ser localizados por meio de links, disponibilizados no Áurea.

Não há prazo específico de guarda para tais documentos, que seguem as regras de temporalidade gerais (Portaria-TCU 110/2020).

As informações pessoais inseridas no Áurea e nos documentos do e-TCU são tratadas exclusivamente para o fim de se verificar o cumprimento das obrigações trabalhistas e previdenciárias das empresas contratadas, segundo as premissas constantes da Portaria-TCU 444/2018. A análise da documentação comprobatória da regularidade é individual.

Ainda no contexto de fiscalização contratual, os dados pessoais dos prestadores de serviços – nome e CPF – também são inseridos, pelos fiscais de contratos, no Sistema de Gestão de Contratos do TCU (Contrata). Os dados permanecem no referido sistema enquanto os prestadores estão vinculados aos contratos objeto de fiscalização. Extinto o vínculo, os dados devem ser excluídos. O propósito do tratamento, nesse caso, é viabilizar o controle de acesso às dependências do órgão e a sistemas corporativos, mormente da área de tecnologia da informação (TI). Em nenhuma hipótese há compartilhamento de dados.

2.2. DESCRIÇÃO DOS TIPOS DE DADOS PESSOAIS COLETADOS E DO MÉTODO DE COLETA DE DADOS

O quadro abaixo sumariza os tipos de dados pessoais coletados e o método de coleta de tais dados.

FASE DO PROCESSO DE CONTRATAÇÃO	CATEGORIA	TIPOS DE DADOS PESSOAIS COLETADOS	MÉTODO DE COLETA DOS DADOS
Licitação	Dados cadastrais do representante da empresa	Nome, CPF e RG	Extração de sistemas governamentais; recebimento via e-mail ou documento encaminhado pela empresa (comunicação, proposta)
Fiscalização	Dados cadastrais do representante da empresa	Nome, CPF e RG	Recebimento via e-mail ou documento encaminhado pela empresa (comunicação, proposta)
	Dados referentes aos funcionários terceirizados, para acompanhamento da conformidade previdenciária, fiscal e trabalhista da empresa	Nome, CPF, RG, carteira de trabalho, exames médicos admissionais e demissionais, cópias de contracheques, comprovantes de transferências bancárias, cópias de extratos do INSS e FGTS, folhas de ponto, avisos de férias, guias de recolhimento do FGTS e GFIPs, além de outros dados enviados pela contratada	Recebimento via e-mail ou documento encaminhado pela empresa (comunicação, proposta) endereçado aos fiscais de contrato

Fonte: Oficina Sesouv-Selip.

2.3. RISCOS NA PROTEÇÃO DE DADOS

Esta sessão cuida da identificação, análise e avaliação dos riscos associados ao tratamento dos dados pessoais nas fases indicadas.

A avaliação é produto da oficina realizada com os especialistas, que atribuíram nota de probabilidade e impacto para cada risco identificado, considerando a escala fornecida. A escala utilizada tem os valores possíveis de 3, 5, 8, 13 e 21, sendo 3 o menor valor a ser atribuído para probabilidade/impacto dos riscos e 21 o maior valor possível de atribuição. Os resultados foram validados em discussões e reflexões em grupo.

Os riscos e seus níveis, após a etapa de avaliação, são descritos abaixo.

Quadro 4 – Níveis de risco à proteção de dados pessoais

RISCO	PROPROBABILIDADE	IMPACTO	NÍVEL DO RISCO
Acesso aos dados pessoais por pessoa não autorizada	13	8	104
Coleta excessiva de dados pessoais (violação ao princípio da necessidade)	13	5	65
Utilização dos dados pessoais para outra finalidade que não a informada ao titular/ prevista em lei (violação ao princípio da adequação)	5	13	65
Vazamento de dados pessoais	5	13	65
Reidentificação de dados anonimizados	8	8	64
Retenção de dados pessoais além do período necessário	21	3	63
Acesso aos dados pessoais fora das hipóteses previstas pela LGPD (finalidade, adequação, necessidade)	5	8	40
Modificação de dados pessoais sem autorização do titular	3	13	39
Apropriação ou uso indevido dos dados pessoais do titular	3	13	39

RISCO	PROPROBABILIDADE	IMPACTO	NÍVEL DO RISCO
Divulgação não autorizada (intencional) de dados pessoais contidos em documentos/ arquivos	3	13	39
Remoção (intencional) não autorizada de dados pessoais	3	8	24
Compartilhamento de dados pessoais fora das hipóteses legais (art. 26 LGPD)	3	8	24
Negativa indevida de acesso aos dados pelo titular	3	5	15
Utilização de informações equivocadas ou desatualizadas no tratamento de dados pessoais	3	3	9

Fonte: Oficina Sesouv-Selip.

Do quadro acima, infere-se que apenas o risco "acesso aos dados pessoais por pessoa não autorizada" representa risco "alto". Os demais apresentam-se como riscos "médios", "baixos" ou "muito baixos".

2.4. MEDIDAS DE SALVAGUARDA E MITIGAÇÃO DE RISCOS

Com os riscos identificados, analisados e avaliados, segue-se a fase de tratamento dos riscos. Como a LGPD expressamente prevê a mitigação dos riscos relacionados à proteção de dados pessoais, tem-se a imposição de implementação de controles internos, ou seja, medidas de salvaguarda para redução e prevenção de tais riscos.

As medidas de salvaguarda em privacidade de dados têm o objetivo de reduzir o nível de risco suportado pelo processo de trabalho. Usualmente, os controles são aplicados somente para os riscos de nível "alto" ou "muito alto". No entanto, os controles relativos à privacidade de dados têm por característica serem transversais, isto é, capazes de mitigar simultaneamente mais de um risco.

Por exemplo, um controle lógico de criptografia tem a capacidade de mitigar não só o risco de acesso aos dados pessoais por pessoa não autorizada, mas também os de vazamento de dados pessoais e divulgação não autorizada desses dados, na medida em que, mesmo que os dados sejam vazados/divulgados, o receptor de tais dados não consegue acessá-los.

Desta forma, apesar de as medidas aqui propostas terem como objetivo principal a mitigação do risco "acesso aos dados pessoais por pessoa não autorizada", considerado neste trabalho como de nível "alto", elas também têm a capacidade de mitigar os demais riscos à proteção de dados pessoais relacionados ao processo de contratação.

Outro fator considerado na proposição dos controles foram as balizas legais que delimitam toda a atividade de contratação e sua correspondência com a base principiológica da LGPD. A lei estabelece, como princípios a serem observados nas atividades de tratamento de dados pessoais, os seguintes:

> "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Resta claro, da observação dos princípios, o fomento ao aspecto preventivo. Essa diretriz norteou as reflexões sobra as medidas de controle.

Por fim, buscou-se compatibilizar as disposições da LGPD com a imprescindibilidade da transparência, especialmente relevante nas atividades relacionadas às contratações públicas. Partiu-se da premissa de que a LGPD, afora não se contrapor à Lei 12.527/2011 – Lei de Acesso à Informação (LAI), orientadora da transparência, a complementa. É esse o entendimento da doutrina especializada[4].

[4]TASSO, op. cit.

> Conforme já consignado, defendemos o caráter de complementariedade e diálogo entre a LAI e a LGPD, seja pela remissão expressa desta àquela, como pela identidade de propósitos das duas leis, qual seja conferir ao Poder Público a mais concreta transparência de sua atividade, permitindo ao cidadão o acesso aos dados do próprio órgão consultado e, agora, às operações de tratamento dos dados pessoais do indivíduo.

Com efeito, deve-se reconhecer que a transparência é princípio orientador da LGPD, e que a LAI já tratava da proteção de dados. "A Lei de Acesso à Informação associa diretamente a proteção de dados pessoais a uma gestão transparente da informação.". [5]

Feitos esses esclarecimentos, passa-se às medidas de controle propostas.

2.4.1. CLASSIFICAÇÃO DA INFORMAÇÃO

A primeira medida de mitigação sugerida é a classificação da informação, que compreende as medidas para restrição de acesso às informações classificadas.

Dados pessoais tratados pelo processo de contratação, como dados bancários de funcionários terceirizados e extratos de INSS e FGTS, são dados relativos à honra, intimidade e vida privada, nos termos do art. 31 da LAI.

[5]BIONI, Bruno Ricardo. Ecologia: uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes?. In: _____ **Proteção de dados** [livro eletrônico]: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

2.4.2. DESCARTE DE DADOS PESSOAIS PELOS FISCAIS DE CONTRATOS E PELA COMISSÃO DE LICITAÇÃO OU PELO PREGOEIRO

Tanto o fiscal de contrato quanto a comissão de licitação ou o pregoeiro recebem dados pessoais durante as fases de fiscalização e licitação do processo licitatório, respectivamente. Aquele com mais frequência.

É comum que tais dados, quando eletrônicos, fiquem armazenados nas máquinas, em dispositivos de memória ou no correio eletrônico.

Após a finalização das atividades, é preciso cautela adicional, para que nenhuma outra pessoa tenha acesso aos dados. A guarda desnecessária contraria o princípio da necessidade, previsto na LGPD, e impõe custos e riscos ao Tribunal.

Nesse sentido, recomenda-se que os documentos físicos que contenham dados pessoais sejam descartados por fragmentadora de papéis e documentos eletrônicos que contenham dados pessoais sejam apagados por meio de softwares específicos, a exemplo do *file shredder*.

2.4.3. REVISÃO DAS REGRAS DE ACESSO AO SISTEMA ÁUREA E A SUAS FUNCIONALIDADES

Por abarcar a etapa de verificação de conformidade previdenciária, fiscal e trabalhista, o sistema Áurea recebe diversos dados pessoais que podem ser visualizados por servidores e colaboradores que têm acesso a ele.

Nesse sentido, sugere-se a revisão das regras de acesso, para evitar que colaboradores eventuais – estagiários, terceirizados, pessoas que já deixaram de ser fiscais de contrato ou servidores que não tenham a incumbência atual de realizar a verificação de conformidade – tenham acesso ilimitado ao sistema e, reflexamente, aos dados pessoais. Pode-se, por exemplo, conceder aos colaboradores perfil de cadastrador, com data de revogação automática.

Como o sistema guarda muitos dados pessoais, alguns sensíveis, é recomendável que o acesso fique restrito ao mínimo necessário à realização do trabalho de fiscalização. Ademais, é prudente que, periodicamente, se realize o controle dos perfis de acesso. Tal medida, inclusive, está sendo gestada, para compor minuta de novo regulamento do Tribunal sobre controle de acesso.

Os dados pessoais de prestadores de serviços são fornecidos pelas empresas contratadas. São enviados por *e-mail* aos fiscais, mediante protocolo, ou até por meio postal. Essa sistemática acaba por fomentar a circulação e o armazenamento indevido de dados, em máquinas, diretórios de rede e e-mails, em desacordo com o princípio da necessidade. É recomendável que a própria empresa contratada possa responsabilizar-se pela inserção dos dados no sistema Áurea. Afora mitigar os riscos associados ao tratamento de dados pessoais, a mudança de procedimento eliminaria a atuação do fiscal de contrato no cadastro dos dados pessoais do sistema, reduzindo uma etapa do processo de trabalho. E ainda teria o potencial de melhorar a qualidade do processo, mitigando a possibilidade de se realizar cadastro intempestivo ou incorreto de dados.

Outra melhoria aconselhável no sistema, e de natureza eminentemente técnica, é implementar a possibilidade de visualização de documentos sem que, para isso, seja necessário realizar *download* na máquina.

2.4.4 FIXAÇÃO DE CRITÉRIOS DE TEMPORALIDADE PARA GUARDA DE DOCUMENTOS ELETRÔNICOS DE FISCALIZAÇÃO DE CONTRATOS NO SISTEMA E-TCU

Os documentos cadastrados no sistema Áurea, ao fim do período de avaliação de regularidade a que se referem, são convertidos em documentos eletrônicos do e-TCU. Trata-se de uma grande massa de documentos, quem contém, inclusive, muitos dados sensíveis.

Considerando que os documentos são coletados para o fim exclusivo de comprovar a regularidade trabalhista e previdenciária das contratadas, findos os respectivos contratos, sua principal utilidade se perde.

A guarda só se justificaria, em tempo excedente à duração do contrato, residualmente, como subsídio à defesa da União em eventual ação trabalhista. Nesse caso, a guarda deveria se limitar ao prazo prescricional para a exigência dos créditos trabalhistas.[6]

Assim, é recomendável que seja estabelecida uma regra de temporalidade específica para os documentos de regularidade, adequada à sua finalidade. Finalizado o prazo, os documentos devem ser descartados das bases de dados.

[6]Segundo o art. 11 da Consolidação das Leis Trabalhistas (CLT), a pretensão prescreve em cinco anos, até o limite de dois anos após a extinção do contrato de trabalho.

2.4.5. EXPEDIÇÃO FORMAL DE ORIENTAÇÃO PARA AGENTES QUE ATUAM NOS PROCESSOS DE CONTRATAÇÃO E GESTÃO CONTRATUAL

É importante que os agentes públicos que atuam nos processos de contratação – fiscais, gestores, equipes de planejamento, comissão de licitação e pregoeiros – sejam orientados e alertados acerca dos cuidados necessários no tratamento de dados pessoais. Além de mitigar riscos, a medida favorece a cultura de proteção de dados pessoais.

Recomenda-se que seja expedida orientação formal da Selip em que constem cuidados e controles no tratamento de dados pessoais, de fácil implementação. A orientação deve ser balizada pelos princípios que regem o tratamento de dados, sobretudo os da finalidade, necessidade e transparência. Nesse sentido, pode-se, por exemplo, instruir os agentes a:

a. reduzir a quantidade de dados pessoais coletados em seus processos de trabalho ao mínimo necessário ao propósito de tratamento;

b. evitar propagar cópias de e-mails que contenham dados pessoais;

c. evitar duplicar e armazenar, sem que seja necessário, documentos que contenham dados pessoais;

d. orientar as empresas contratadas a encaminhar somente os documentos dos prestadores de serviços alocados aos contratos fiscalizados;

e. dispensar dados pessoais em documentos e informações que não sejam absolutamente necessários;

f. estabelecer rotinas de controle de acompanhamento dos vínculos contratuais e descarte de registros de dados pessoais do sistema Contrata, de modo que nele não fiquem armazenados dados desnecessários.

Outras medidas, objeto de orientação, podem ser avaliadas, em conjunto com a Sesouv ou com as unidades responsáveis pela área de TI do Tribunal. Cita-se, como exemplo, a possiblidade de que os agentes sejam instruídos a intensificar o uso de soluções já contratadas e disponíveis, como a criptografia nas mensagens de *e-mail*.

2.4.6. PADRONIZAÇÃO DE CLÁUSULAS CONTRATUAIS QUE ESTABELEÇAM A OBRIGAÇÃO DE AS EMPRESAS TERCEIRIZADAS ENVIAREM OS DADOS PESSOAIS AO TCU DE FORMA CRIPTOGRAFADA E CONTENDO EXCLUSIVAMENTE OS DADOS DE FUNCIONÁRIOS EM EXERCÍCIO NO TCU

A criptografia restringe o acesso aos dados pessoais enviados pelas empresas apenas ao portador da chave de criptografia, o que mitiga o risco de acessos indesejados.

Além disso, identificou-se que as empresas contratadas costumeiramente enviam ao TCU dados pessoais de todos os funcionários terceirizados que ela emprega, não apenas os vinculados aos contratos objeto da fiscalização. Essa prática fere os princípios da necessidade e finalidade e aumenta o risco da privacidade de dados. É recomendável que a obrigação de enviar somente os dados necessários conste expressamente do contrato, inclusive associando-se a ela punições proporcionais, para o caso de descumprimento.

2.5. AVALIAÇÃO DAS MEDIDAS DE MITIGAÇÃO DE RISCOS

As medidas de mitigação dos riscos concentraram-se na fase de fiscalização dos contratos. É acertada essa orientação, porquanto reside nessa fase os riscos mais sensíveis associados à proteção de dados. Há que se considerar, ainda, que, diversamente do que ocorre na fase do processo licitatório, não se trata de dados públicos, submetidos a controle social.

De toda forma, algumas medidas de controle aventadas, dado seu efeito transversal, alcançam os dados pessoais tratados em processos licitatórios, de modo que se espera, também em relação a eles, a prevenção e redução de riscos.

Os controles propostos são, em geral, de fácil implementação e baixo custo. Alguns já são utilizados ou passíveis de utilização imediata. Ademais, não implicam restrições à transparência, princípio do qual as atividades de contratação não podem se afastar.

Passa-se a algumas considerações individuais sobre os controles propostos.

2.5.1. CLASSIFICAÇÃO DA INFORMAÇÃO

No âmbito da Secretaria-Geral de Administração (Segedam), no decorrer do exercício de 2020, foi desenvolvido o Projeto Classificar, com o objetivo de implementar a classificação de informações na unidade. O projeto foi tratado no TC-010.322/2020-5.

As etapas iniciais geraram, como produtos, manuais de classificação de informações e modelos de atos classificatórios das informações dos processos administrativos sob responsabilidade, respectivamente, da Selip e Secretaria de Gestão de Pessoas (Segep).

Na etapa final do projeto, houve a coordenação e o acompanhamento da implantação dos procedimentos de classificação da informação propostos à Selip, bem como a organização e disponibilização, em sítio eletrônico, dos produtos entregues no âmbito do projeto. Os produtos gerados no âmbito do projeto foram disponibilizados e organizados na wiki Classificação da Informação, na Segedam.

Após os trabalhos conduzidos no âmbito do Projeto Classificar, foi possível concluir, entre outras constatações, que o sistema e-TCU Administrativo carece de funcionalidades, para atender os requisitos de classificação das informações nos moldes da LAI.

Desta forma, para que o controle proposto possa ser adotado de forma mais efetiva, de modo a não implicar entrave nos processos de trabalho, são necessárias adequações no e-TCU.

Dada a importância da medida, que tem efeitos, também, no pleno cumprimento da LAI, propõe-se que seja expedida determinação à Secretaria de Soluções de Tecnologia da Informação (STI), acompanhada de cópia deste relatório, para que avalie a demanda de alterações no sistema e, a depender da viabilidade da medida, a inclua em seu planejamento operacional.

2.5.2. DESCARTE DE DADOS PESSOAIS PELOS FISCAIS DE CONTRATOS E PELA COMISSÃO DE LICITAÇÃO OU PELO PREGOEIRO

Quanto ao descarte físico de documentos, não há óbice a que seja de pronto implementada a rotina. Na verdade, já existe orientação nesse sentido, que pode ser reforçada.

No entanto, quanto aos softwares específicos para descarte de documentos eletrônicos, deve ser avaliada a viabilidade técnica da medida e sua compatibilidade com as demais ferramentas e funcionalidades de TI existentes, o que só pode ser feito pela área competente, a Secretaria de Infraestrutura e Tecnologia da Informação (Setic). A unidade também é a responsável pelo processo de aquisição do software, caso seja essa a solução eleita.

Logo, recomenda-se que seja remetida cópia deste relatório à Setic, para que avalie a viabilidade técnica de aquisição de *software* de descarte de documentos eletrônicos ou disponibilização nas máquinas, caso já exista, a depender da avaliação, ainda que a unidade inclua a demanda em seu planejamento de aquisições.

2.5.3. REVISÃO DAS REGRAS DE ACESSO AO SISTEMA ÁUREA E A SUAS FUNCIONALIDADES

Os controles propostos mostram-se oportunos. Não há embaraço a que as regras de acesso sejam de pronto alteradas, na forma sugerida, para que seja reduzido o acesso aos dados pessoais armazenados no sistema.

Quanto à melhoria técnica consistente na possibilidade de visualização de documentos sem que, para isso, seja necessário realizar download da máquina, depende de avaliação e atuação da Adgedam, unidade que detém competência para realizar tais espécies de alterações técnicas nos sistemas administrativos.

Propõe-se, portanto, que seja expedida determinação à Diretoria de Planejamento e Gestão de Contratações (Diplag/Selip), para que implemente as regras de controle de acesso no sistema *Áurea*, bem como à Adgedam, para que avalie a viabilidade técnica de alteração do sistema, consistente em possibilitar a visualização de documentos sem *download*. Caso a unidade conclua pela viabilidade da medida, que inclua em seu planejamento a correspondente ação.

É recomendável, ainda, que regras fiquem descritas em local próprio e acessível às unidades interessadas.

2.5.4. FIXAÇÃO DE CRITÉRIOS DE TEMPORALIDADE PARA GUARDA DE DOCUMENTOS DE FISCALIZAÇÃO DE CONTRATOS NO SISTEMA E-TCU

A medida proposta tem potencial de mitigar risco relevante, tendo em vista o volume de dados pessoais constantes dos documentos. Além disso, reduz a massa documental gerida pelo TCU.

Dada a natureza da matéria em discussão – classificação de temporalidade de documentos –, na forma do art. 4° da Portaria-TCU 110/2020, propõe-se que seja determinado à Comissão Permanente de Avaliação de Documentos (CAD) que analise a medida, em conjunto, no que for cabível, com a STI e Selip.

2.5.5. EXPEDIÇÃO FORMAL DE ORIENTAÇÃO PARA AGENTES QUE ATUAM NOS PROCESSOS DE CONTRATAÇÃO E GESTÃO CONTRATUAL

A medida é simples, de pouco custo e tem potencial de alcançar bons resultados. Não há impedimento a que seja imediatamente adotada.

Assim, recomenda-se que seja determinado à Selip que providencie a orientação, na forma proposta. Deve a unidade valer-se do apoio da Sesouv ou de outras unidades técnicas, caso julgue necessário.

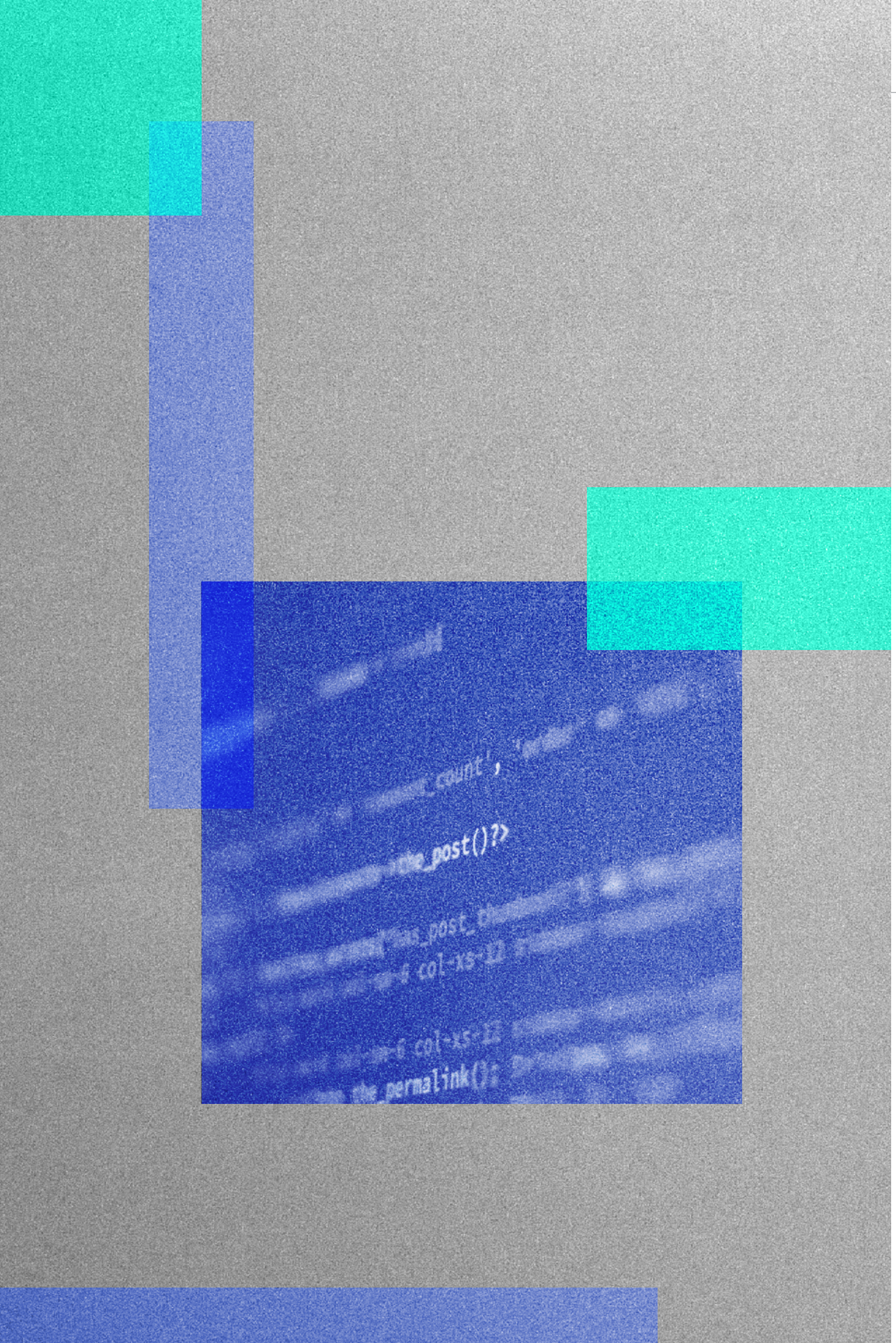
2.5.6. PADRONIZAÇÃO DE CLÁUSULAS CONTRATUAIS QUE ESTABELECEM A OBRIGAÇÃO DE AS EMPRESAS TERCEIRIZADAS ENVIAREM OS DADOS PESSOAIS AO TCU DE FORMA CRIPTOGRAFADA E CONTENDO EXCLUSIVAMENTE OS DADOS DE FUNCIONÁRIOS EM EXERCÍCIO NO TCU

Já consta dos planos operacionais da Sesouv e Selip ação conjunta, com o propósito de realizar a alteração nos modelos de contratos, para que contemplem a cláusula proposta. Trata-se da ação 33 – Coordenar a Criação de Cláusula Padrão sobre Proteção de Dados na Selip, lançada no sistema Planejar sob o código 4659, com data de conclusão prevista para o dia 30/3/2022.

Embora a ação já conste dos planos, cabe ressaltar que sua efetiva execução depende de prévia avaliação de natureza técnica, consistente na análise da viabilidade e dos meios de adoção da solução de criptografia. Portanto, a medida não prescinde de apoio da Setic.

Assim, recomenda-se que seja determinado à Setic que estude a viabilidade da medida e adote as ações técnicas necessárias para implementá-la, a depender dos resultados do estudo.

Recomenda-se, ainda, que seja determinado à Selip que providencie a inclusão, em suas minutas contratuais padronizadas, após a finalização da aludida ação, de cláusulas contratuais que estabeleçam a obrigação de as empresas terceirizadas enviarem os dados pessoais ao TCU de forma criptografada e contendo exclusivamente os dados de funcionários em exercício no TCU.



3. CONCLUSÕES E ENCAMINHAMENTO

Este relatório tratou de medidas de proteção de dados em um contexto delimitado – os principais processos de trabalho relacionados às contrações realizadas pelo TCU.

Muito embora os controles propostos, e os já operantes, tenham efeitos transversais, não há impedimento a que os riscos associados a outros processos relacionados às contratações sejam também avaliados e tratados de modo mais pontual. Ou, ainda, que processos de trabalho diversos tenham os riscos à proteção de dados pessoais mitigados, por meio de premissas e metodologia semelhantes às utilizadas para produção deste relatório.

De toda forma, é imprescindível que as ações destinadas à proteção de dados pessoais sejam contínuas, consistentes e abrangentes. Isso exige monitoramento, reavaliação permanente e capacidade de inovação. As práticas, a exemplo das propostas neste relatório, devem estar inseridas em um sistema de governança eficiente e integrado. Não é demais lembrar, a esse propósito, que a LGPD dedicou sessão específica para tratar das Boas Práticas e da Governança, o que reforça a responsabilidade atribuída às instituições na garantia da proteção aos dados pessoais, agora direito fundamental expressamente consagrado na Constituição federal.

Essa conjuntura sustenta a relevância dos controles propostos neste documento, que deve ser tido como parte de um arranjo maior e permanente de gestão de riscos em proteção de dados.

Feitas essas considerações, submete-se este relatório à Presidência, para que avalie as medidas propostas e, se julgar cabível, faça os encaminhamentos indicados.

Cabe, por fim, observar, quanto ao encaminhamento das medidas, que se trata de encargo próprio do controlador de dados pessoais. Segundo orientação publicada pela Autoridade Nacional de Proteção de Dados (ANPD)[7].

> (...) a LGPD atribuiu aos órgãos públicos obrigações típicas de controlador, indicando que, no setor público, essas obrigações devem ser distribuídas entre as principais unidades administrativas despersonalizadas que integram a pessoa jurídica de direito público e realizam tratamento de dados pessoais.
>
> 22. Nesse sentido, a União, como controladora, é a responsável perante a LGPD, mas as atribuições de controlador, por força da desconcentração administrativa, são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte, fenômeno que caracteriza a distribuição interna das competências.

Desta forma, embora seja a União, em última análise, a responsável pelas obrigações decorrentes da LGPD, são atribuídas ao TCU as obrigações típicas de controlador, razão pela qual se entende necessária a remessa do relatório à avaliação da Presidência.

[6]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília, maio de 2021.

Responsabilidade pelo conteúdo
Secretaria de Licitações, Contratos e Patrimônio (Selip)
Secretaria de Ouvidoria e Segurança da Informação (Sesouv)

Projeto gráfico, diagramação e capa
Secretaria de Comunicação (Secom)
Núcleo de Criação e Editoração (NCE)

Tribunal de Contas da União
Secretaria-Geral da Presidência (Segepres)
SAFS Quadra 4 Lote 1
Edifício Sede Sala 146
70.042-900, Brasília – DF
(61) 3316-5338
segepres@tcu.gov.br

Ouvidoria do TCU
0800 644 1500
ouvidoria@tcu.gov.br

Impresso pela Senge/Segedam

MISSÃO

APRIMORAR A ADMINISTRAÇÃO PÚBLICA EM BENEFÍCIO DA SOCIEDADE POR MEIO DO CONTROLE EXTERNO.

VISÃO

SER REFERÊNCIA NA PROMOÇÃO DE UMA ADMINISTRAÇÃO PÚBLICA EFETIVA, ÉTICA, ÁGIL E RESPONSÁVEL.

TRIBUNAL DE CONTAS DA UNIÃO