TRT-4ª REGIÃO
Secretaria de Auditoria

RELATÓRIO FINAL DE AUDITORIA

AUDITORIA NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

JULHO/2026

TRT-4ª REGIÃO
Secretaria de Auditoria

DA AUDITORIA

Modalidade: Conformidade

Relatório nº: 01/2026

PROAD nº: 700/2026

Objeto da auditoria: Medidas adotadas para implementação da Lei Geral de Proteção de Dados no âmbito do TRT4.

Objetivo da auditoria: Avaliar as medidas implementadas pelo TRT4 para adequação à Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais – LGPD, por meio da aplicação de questionários disponibilizados pelo Tribunal de Contas da União (TCU).

Integrantes da auditoria: Adriano Prado Cavalheiro (Equipe de Auditoria)
Pérola Priscila da Silva Rocha (Equipe de Auditoria)
José Cláudio da Rosa Riccardi (Auditor Responsável)
Carolina Feuerharmel Litvin (Supervisora)

DA UNIDADE AUDITADA

Unidade auditada: **Subcomitê de Proteção de Dados Pessoais**

Responsável pela unidade auditada:

Nome: Desembargador Presidente Alexandre Corrêa Da Cruz
Função: Coordenador do Subcomitê de Proteção de Dados Pessoais
Período: desde 05.12.2025 (Termo de Posse nº 03/2025 – PROAD nº 8148/2025)

SUMÁRIO EXECUTIVO

O QUE FOI AUDITADO?

A presente auditoria teve como objetivo avaliar as medidas implementadas pelo TRT4 para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), bem como a efetividade das práticas operacionais já adotadas em matéria de proteção de dados pessoais. O escopo do trabalho foi delimitado a partir da Matriz de Planejamento e do questionário elaborados pela Unidade de Auditoria em Tecnologia da Informação do Tribunal de Contas da União, adaptados à realidade institucional deste Tribunal.

POR QUE ESTE TRABALHO FOI REALIZADO?

Este trabalho foi selecionado para compor o Plano Anual de Auditoria – Exercício 2026 em atendimento à recomendação do item 9.1.8.2 do Acórdão TCU nº 1.372/2025 – Plenário, que orientou o envolvimento das unidades de auditoria interna no processo de adequação dos órgãos à LGPD. O trabalho está alinhado ao Plano Estratégico Institucional 2021-2026, especialmente aos seguintes objetivos: nº 7 – Fortalecer a Governança e a Gestão Estratégica e nº 10 – Aprimorar a Governança de Tecnologia da Informação e Comunicação e a Proteção de Dados.

QUAIS FORAM AS CONCLUSÕES E AS PROPOSTAS DE ENCAMINHAMENTO?

A auditoria concluiu que o TRT4 vem adotando medidas relevantes para a implementação da LGPD e demonstrando comprometimento institucional com a proteção de dados pessoais. Embora a maior parte dos procedimentos avaliados tenha apresentado aderência aos critérios normativos adotados no trabalho, foram identificadas oportunidades de melhoria cuja implementação contribuirá para o fortalecimento da conformidade normativa, da gestão de riscos e dos controles relacionados ao tratamento de dados pessoais. Em decorrência das análises realizadas, foram apresentadas cinco propostas de encaminhamento:

R1. Promover **ações de conscientização e de capacitação** em proteção de dados pessoais, especialmente para magistrados(as) e servidores(as) que desempenham atividades críticas relacionadas ao tratamento de dados pessoais, considerando os diferentes níveis de responsabilidade e atribuições exercidas.

R2. Dar continuidade e ampliar gradualmente a **elaboração dos Inventários de Dados Pessoais (IDP)** para os processos de trabalho ainda não mapeados e para as demais unidades administrativas do Tribunal.

R3. Adotar mecanismos de controle para assegurar o **preenchimento adequado dos campos obrigatórios e a consistência das informações registradas nos IDPs**, especialmente aquelas relacionadas ao prazo de retenção dos dados pessoais.

R4. Promover a **elaboração gradual de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD)** para operações de tratamento que apresentem maior potencial de impacto aos titulares, especialmente aquelas que envolvam elevado volume de dados pessoais, dados pessoais sensíveis ou dados de crianças e adolescentes.

R5. Realizar o **gerenciamento dos riscos** associados ao **armazenamento de dados pessoais em serviços de nuvem**.

QUAIS OS PRÓXIMOS PASSOS?

Após a decisão da Presidência acerca deste Relatório, a Secretaria de Auditoria realizará o monitoramento das propostas de encaminhamento acolhidas.

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Agência Nacional de Proteção de Dados
CNJ	Conselho Nacional de Justiça
CSJT	Conselho Superior da Justiça do Trabalho
DIRAUD-Jud	Diretrizes Técnicas das Atividades de Auditoria Interna Governamental do Poder Judiciário
DG	Diretoria-Geral
DGD	Divisão de Governança de Dados
Ejud4	Escola Judicial do TRT da 4ª Região
GP	Gabinete da Presidência
CGPD	Comitê Gestor de Proteção de Dados Pessoais
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IDP	Inventário de Dados Pessoais
ISO	*International Organization for Standardization*
IEC	*International Electrotechnical Commission*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira Registrada
PAC	Plano Anual de Capacitação
PAS	Portal de Apoio ao SIGEP-JT
PROAD	Processo Administrativo Eletrônico (Sistema PROAD-OUV)
PSI	Política de Segurança da Informação
RA	Resolução Administrativa
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
RDI	Requisição de Documentos e Informações
SaaS	*Software as a Service* (Software como Serviço)
SA	Secretaria de Administração
Seama	Secretaria de Apoio aos Magistrados
Seaudi	Secretaria de Auditoria
Secof	Secretaria de Orçamento e Finanças

Secom	Secretaria de Comunicação Social
SecServ	Secretaria de Serviços
Segesp	Secretaria de Gestão de Pessoas
Sempro	Secretaria de Manutenção e Projetos
SeSaúde	Secretaria de Saúde e Assistência
SIGEP-JT	Sistema Integrado de Gestão de Pessoas da Justiça do Trabalho
SILC	Sistema de Licitações e Contratos
SGTI	Secretaria-Geral de Tecnologia e Inovação
TCU	Tribunal de Contas da União
TRT4	Tribunal Regional do Trabalho da 4ª Região
TST	Tribunal Superior do Trabalho

SUMÁRIO

1. INTRODUÇÃO

1.1. APRESENTAÇÃO

A presente auditoria foi incluída no Plano Anual de Auditoria – Exercício 2026, conforme registrado no PROAD nº 7070/2025, em atendimento à recomendação contida no item 9.1.8.2 do Acórdão TCU nº 1.372/2025 – Plenário. Nesse Acórdão, a Corte de Contas recomendou que a Unidade de Auditoria Interna do Tribunal fosse envolvida no processo de adequação do TRT4 à Lei Geral de Proteção de Dados (LGPD), avaliando e monitorando os riscos relacionados à privacidade e à proteção de dados pessoais.

O trabalho alinha-se ao Planejamento Estratégico Institucional do TRT4 – 2021–2026) e ao Plano Diretor de Tecnologia da Informação e Comunicação – 2024–2026), especialmente no que se refere aos objetivos estratégicos relacionados à governança, à integridade, à segurança da informação, à gestão de riscos e à confiabilidade dos sistemas institucionais na proteção de dados tratados pelo Tribunal. Como exemplo, destacam-se os seguintes objetivos do PEI 2021-2026: #7 Fortalecer a Governança e a Gestão Estratégica e #10 Aprimorar a Governança de Tecnologia da Informação e Comunicação – TIC e a Proteção de Dados.

A realização deste trabalho também decorre da crescente relevância atribuída à **proteção de dados pessoais no âmbito da Administração Pública**, especialmente após a entrada em vigor da Lei nº 13.709/2018 (LGPD). Além disso, o Conselho Nacional de Justiça (CNJ), o Conselho Superior da Justiça do Trabalho (CSJT) e o Tribunal de Contas da União (TCU) têm intensificado ações de controle e monitoramento de forma a impulsionar o cumprimento dessa lei pelos órgãos públicos.

Nesse contexto, o CNJ e o CSJT editaram atos específicos voltados à governança e à proteção de dados pessoais no âmbito do Poder Judiciário, reforçando a obrigatoriedade de avaliações periódicas de conformidade pelos tribunais – Resolução CNJ nº 363/2021 e Resolução CSJT nº 309/2021, respectivamente. O CSJT realiza periodicamente a análise da maturidade dos Tribunais Regionais do Trabalho quanto à aderência à LGDP por meio do Índice de

Adequação à LGPD. O TCU, por sua vez, realizou a Auditoria de Conformidade, no exercício de 2024, no âmbito do processo TC 009.980/2024-5, que avaliou o nível de adequação dos órgãos públicos federais à LGPD, tendo o TRT4 participado do levantamento e recebido Relatório de Feedback individualizado, em 2025. Esse trabalho estabeleceu critérios objetivos de conformidade, estruturados em dimensões de governança, controles, segurança da informação, transparência e direitos dos titulares de dados, constituindo referencial técnico e metodológico consolidado para avaliações de conformidade à LGPD no setor público (Painel Nacional de Implementação da LGPD).

Nesse cenário, esta auditoria justifica-se pela necessidade de verificar a aderência atual do Tribunal às exigências normativas e às recomendações e determinações do TCU, de modo a apoiar a Administração com um diagnóstico objetivo e contribuir para o fortalecimento da governança, da transparência e da proteção dos direitos dos titulares de dados pessoais tratados pelo TRT4.

1.2. VISÃO GERAL DO OBJETO

A LGPD estabeleceu um novo marco legal para o **tratamento de dados pessoais**[1] no Brasil, aplicável tanto a pessoas naturais quanto a pessoas jurídicas de direito público e privado. A norma impõe aos órgãos públicos o dever de instituir estruturas de governança, políticas, controles e mecanismos de responsabilização capazes de assegurar o tratamento adequado, seguro e transparente dos dados pessoais sob sua custódia.

No âmbito do Poder Judiciário, Teixeira e Guerreiro (2022, p. 74)[2] destacam:

> Em casos de exercício regular de direito em um processo judicial, administrativo ou arbitral, poderá haver o tratamento de dados pessoais, **mesmo sem o consentimento do titular**, como, por exemplo, para fornecer os dados pessoais de uma testemunha ou de um réu para o ajuizamento de uma ação ou a juntada de provas que contenham dados pessoais. (grifo nosso)

[1] "Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do *Internet Protocolo* (IP), dados acadêmicos, entre outros. Sempre relacionados à pessoa natural viva." (PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: comentários à Lei nº 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020. p. 35-36).

[2] TEIXEIRA, Tarcisio; GUERREIRO, Ruth Maria. Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo – 4ª edição. São Paulo: SaraivaJur, 2022.

Nesses casos, o tratamento é fundamentado pelo cumprimento de obrigações legais, seguindo os ritos processuais estabelecidos no Código de Processo Civil e, no caso da Justiça do Trabalho, da Consolidação das Leis Trabalhistas. Cita-se, ainda, o inciso LX do artigo 5º da Constituição Federal que determina que "a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem".

Assim, a **publicidade** constitui a regra no processo judicial, sendo sua restrição a exceção, aplicada apenas nas hipóteses previstas em lei. Esse entendimento também está presente na Resolução CNJ nº 121/2010, que dispõe sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores, expedição de certidões judiciais e dá outras providências:

> Art. 1.º A consulta aos dados básicos dos processos judiciais será disponibilizada na rede mundial de computadores (internet), **assegurado o direito de acesso a informações processuais a toda e qualquer pessoa, independentemente de prévio cadastramento ou de demonstração de interesse**.
> Parágrafo único. **No caso de processo em sigilo ou segredo de justiça não se aplica o disposto neste artigo**. (grifo nosso)

Com relação às atividades exercidas pelo Poder Judiciário no exercício de suas funções administrativas, Cueva (2020, p.209)[3] destaca que:

> No âmbito das **atividades administrativas praticadas pelo Poder Judiciário**, que não se confunde com sua atividade jurisdicional, **o tratamento de dados pessoais deve necessariamente levar em consideração as exigências da** Lei de Acesso à Informação (LAI) quanto à transparência em favor do interesse público, como expressamente previsto na **Lei Geral de Proteção de Dados (LGPD)**. Os dois diplomas, apesar dos enfoques diversos, são harmônicos e compatíveis. (grifo nosso)

No âmbito do TRT4, a **governança de proteção de dados** insere-se em um ambiente organizacional complexo, caracterizado pela pluralidade de unidades administrativas e judiciárias, pela diversidade de sistemas de informação e pela execução de atividades que envolvem o tratamento contínuo de dados pessoais, inclusive dados sensíveis. Essa configuração evidencia a transversalidade do tema e a necessidade de coordenação entre áreas técnicas e de negócio para assegurar a

[3] CUEVA, Ricardo Villas Bôas. A Incidência da Lei Geral de Proteção de Dados Pessoais nas Atividades do Poder Judiciário. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel. (org.). **Lei geral de proteção de dados (Lei nº 13.709/2018) – A caminho da efetividade: contribuições para implementação da LGPD**. São Paulo: Thomson Reuters Brasil, 2020. p. 199-210.

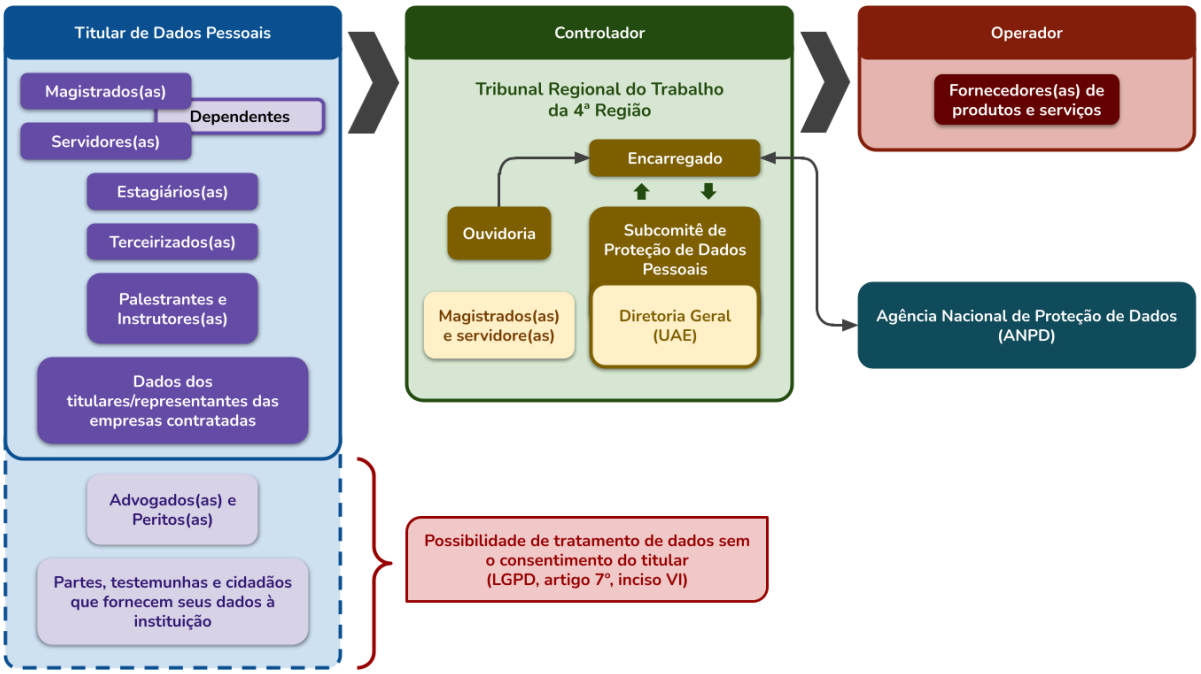
conformidade normativa e a adequada gestão dos riscos associados ao tratamento de dados pessoais.

Conforme destaca Basílio (2023, p. 70)[4]:

> O grande desafio da implantação da LGPD baseia-se justamente na adequação às exigências legais que terminam o manuseio de dados pessoais; estes deverão seguir um cumprimento gerencial a fim de **englobar não somente o departamento de tecnologia da informação, mas sim todos os colaboradores envolvidos**, que precisam compreender como funciona a conjuntura legal adotada no que se refere ao tratamento de dados pessoais de seus clientes. (grifo nosso)

A Figura 1 ilustra os diferentes atores que atuam na implementação da Lei Geral de Proteção de Dados no TRT4.

Figura 1: Atores envolvidos na implementação da LGPD no TRT4



Fonte: Elaboração própria

Os **titulares de dados pessoais** são as pessoas naturais a quem se referem os dados que são objeto de tratamento, constituindo o centro de proteção da LGPD e os(as) destinatários(as) dos direitos assegurados na legislação.

O **controlador** é a pessoa jurídica de direito público responsável por tomar as decisões referentes ao tratamento de dados pessoais e por definir a finalidade desse tratamento. O Tribunal, enquanto órgão do Poder Judiciário da União, exerce o papel de controlador dos dados pessoais tratados no âmbito de suas atividades

[4] BASÍLIO, Cristiane Reis de Amorim. Os desafios da adequação à LGPD: uma análise sobre a aplicação da autodeterminação informativa. São Paulo: Dialética, 2023.

jurisdicionais e administrativas, consoante disposto na Portaria GP.TRT4 nº 2.036/2021. Já o **encarregado** é "Pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional" (PINHEIRO, 2020, p.37)[5]. No TRT4, o juiz Ricardo Fioreze é o Encarregado pelo Tratamento de Dados Pessoais, consoante disposto na Portaria GP.TRT4 nº 2.985/2025.

Como instância interna de apoio à governança de proteção de dados, o TRT4 conta com o **Subcomitê de Proteção de Dados Pessoais**, instituído por meio da Portaria GP.TRT4 nº 4.502/2022. Compete ao referido colegiado propor políticas, estratégias e metas para a conformidade do órgão às disposições da LGPD, bem como prestar orientações e auxílio ao encarregado nas questões relacionadas ao tratamento e à proteção de dados pessoais. A **Ouvidoria** do Tribunal é a unidade responsável pelo recebimento das demandas relacionadas à LGPD.

A **Diretoria-Geral** atua como **Unidade de Apoio Executivo** do Subcomitê de Proteção de Dados Pessoais, exercendo funções essenciais para a organização, funcionamento e transparência do colegiado, estando suas responsabilidades elencadas na Portaria GP.TRT4 nº 4.502/2022.

Ressaltam-se, ainda, **os(as) magistrados(as) e os(as) servidores(as)** das diversas unidades do Tribunal, que executam o tratamento de dados pessoais no exercício de suas atribuições institucionais e que devem observar os princípios previstos na LGPD, as bases legais aplicáveis e as medidas técnicas e administrativas de segurança estabelecidas. Não são considerados controladores ou operadores para fins da LGPD, pois atuam sob o poder diretivo do controlador (BRASIL, 2022)[6].

Os **operadores** são as pessoas naturais ou jurídicas, de direito público ou privado, **externas ao quadro funcional da instituição**, que realizam operações de tratamento de dados pessoais em nome do controlador (artigo 18 da Portaria GP.TRT4 nº 2.036/2021).

---

[5] PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: comentários à Lei nº 13.709/2018 (LGPD). – 2ª edição. São Paulo: Saraiva Educação, 2020.

[6] BRASIL. Agência Nacional de Proteção de Dados (ANPD). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Portal ANPD, 2022. Disponível em https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em 16 jun. 2026.

Por fim, destaca-se a **Agência Nacional de Proteção de Dados (ANPD)**, autarquia especial vinculada ao Ministério da Justiça e Segurança Pública, que é o órgão central de interpretação da LGPD no Brasil e que possui como missão institucional zelar pelo direito de todo cidadão à proteção de seus dados pessoais[7].

No que se refere à implementação da Lei Geral de Proteção de Dados no âmbito do TRT4, observa-se que este Tribunal vem adotando medidas relevantes desde a publicação da lei e das normas do CNJ e do CSJT. Atualmente, a instituição dispõe de normativos que estruturam e regulamentam o tratamento de dados pessoais, como a Portaria GP.TRT4 nº 2.697/2025, que institui a Política de Segurança da Informação, e a Portaria GP.TRT4 nº 2.036/2021, que trata da Política de Privacidade e Proteção de Dados Pessoais. Além disso, há um Programa Institucional de Governança em Privacidade de Dados disponível no site institucional.

A governança institucional relacionada à proteção de dados conta com a participação ativa do Encarregado pelo Tratamento de Dados Pessoais, do Subcomitê de Proteção de Dados Pessoais e da Diretoria-Geral. Ao longo de 2025, o Subcomitê publicou diversas atas que demonstram sua atuação contínua e sistemática no acompanhamento da implementação da LGPD no Tribunal. As reuniões registradas nesse período evidenciam avanços, deliberações relevantes e o monitoramento de temas críticos relacionados à proteção de dados.

Além das normas internas, destacam-se os seguintes pontos importantes na implementação da LGPD no TRT4:

- Criação de uma Página no site institucional sobre a Lei Geral de Proteção de Dados;
- **Inventário de Dados Pessoais – IDP**: realização do mapeamento de dados pessoais em cerca de 40 processos vinculados às Secretarias da Diretoria-Geral;
- **Levantamento dos contratos relacionados a dados pessoais**: elaboração de cláusulas gerais e adequação de editais e contratos à Lei nº 13.709/2018, à Política de Privacidade e Proteção de Dados Pessoais do Tribunal e aos demais normativos aplicáveis;

[7] Planejamento Estratégico ANPD 2024-2027. Acesso em 25 fev. 2026.

- **Comunicação de Incidentes de Segurança à ANPD**: elaboração de modelo de formulário para comunicação de incidentes envolvendo dados pessoais.

1.3. OBJETIVOS E ESCOPO DA AUDITORIA

O objetivo geral desta auditoria é avaliar as medidas implementadas pelo TRT4 para adequação à LGPD, por meio da aplicação de questionário disponibilizado pelo TCU.

A Matriz de Planejamento e o questionário da auditoria, elaborados pela equipe da Unidade de Auditoria Especializada em Tecnologia da Informação do TCU, são apresentados nos Apêndices A e D, respectivamente, do Relatório de Fiscalização. Assim, a delimitação do escopo deste trabalho partiu desses instrumentos de fiscalização do TCU, com as devidas adaptações à realidade deste Tribunal. Importa mencionar que alguns procedimentos de auditoria não foram incorporados ao Programa de Auditoria, tendo em vista que já foram colhidas evidências de seu cumprimento pelo TRT4 na etapa de análise preliminar do objeto (por exemplo: Política de Segurança da Informação e nomeação de encarregado pelo tratamento de dados pessoais).

O questionário do TCU foi composto por duas questões, divididas em 16 subquestões. Além disso, o questionário foi organizado em nove dimensões, agrupadas em dois eixos, sendo um eixo para cada questão de auditoria. Na Figura 2 são apresentados os dois eixos e suas respectivas dimensões.

Figura 2: Eixos e dimensões do questionário do TCU

Fonte: Adaptado do relatório de fiscalização do TCU[8].

[8] BRASIL. Tribunal de Contas da União. Relatório de fiscalização: controles implementados para adequação à LGPD, TC nº 009.980/2024-5. Brasília: TCU, 2024. Acesso em 18 fev. 2026.

1.4. QUESTÕES DE AUDITORIA

As questões de auditoria, elaboradas com base no questionário do TCU, foram as seguintes:

Q1. As iniciativas adotadas para adequação à LGDP, no âmbito do TRT4, atendem ao disposto na legislação?

Q2. A implementação de medidas e controles de proteção de dados pessoais, no âmbito do TRT4, atendem ao disposto na LGPD e demais normas aplicáveis?

Para cada questão de auditoria foram elaboradas subquestões que avaliam os assuntos apresentados, conforme detalhado no quadro a seguir.

Quadro 1 – Principais pontos avaliados nas subquestões de auditoria

Questão	Principais Pontos Avaliados nas Subquestões de Auditoria

Q1	• **Liderança**: elaboração de políticas relacionadas ao tratamento de dados pessoais;
	• **Preparação**: iniciativas para providenciar a adequação do Tribunal à LGPD;
	• **Capacitação**: iniciativas para conscientização e capacitação dos(as) magistrados(as) e dos(as) servidores(as) em proteção de dados pessoais;
	• **Contexto Organizacional**:
	  ○ identificação das principais partes interessadas relacionadas à proteção de dados pessoais do Tribunal;
	  ○ identificação dos dados pessoais que são tratados pelo TRT4, bem como os processos que realizam esses tratamentos.

Q2	• **Conformidade do Tratamento**: conformidade do tratamento de dados pessoais com a LGPD; • **Compartilhamento de Dados Pessoais**: eventual transferência, compartilhamento ou tratamento conjunto de dados; • **Direitos do Titular**: mecanismos disponibilizados para informar e dar atendimento aos direitos dos titulares de dados; • **Violação de Dados Pessoais**: mecanismos para o tratamento de violações de dados pessoais; • **Medidas de Proteção**: medidas instituídas para o tratamento de riscos relacionados à proteção de dados pessoais.

1.5. METODOLOGIA UTILIZADA E LIMITAÇÕES À AUDITORIA

Os trabalhos foram realizados em conformidade com a Resolução CNJ nº 309/2020, que aprova as Diretrizes Técnicas das Atividades de Auditoria Interna Governamental do Poder Judiciário – DIRAUD-Jud e dá outras providências, e com a Portaria GP.TRT4 nº 3.215/2024, que regulamenta a atividade de auditoria desenvolvida pela Secretaria de Auditoria do Tribunal Regional do Trabalho da 4ª Região.

As técnicas de auditoria utilizadas pela equipe para obtenção das informações necessárias à análise do objeto foram: (i) análise documental de documentos compartilhados pela área e de documentos obtidos em consulta ao Sistema de Processo Administrativo Virtual e Ouvidoria (PROAD-OUV) e Sistema Integrado de Licitações e Contratos (SILC); (ii) exame de registros, por meio de consulta às informações constantes no sistema Portal de Apoio ao SIGEP (PAS); (iii) aplicação de questionário, por meio de Requisição de Documentos e Informações (RDI); e (iv) realização de entrevista com outras áreas técnicas para o entendimento de processo relacionado ao objeto deste trabalho e esclarecimento das dúvidas da equipe.

Não foram verificadas dificuldades ou restrições na aplicação dos procedimentos de auditoria, sendo a equipe de auditoria prontamente atendida pela área técnica em todas as requisições formuladas.

Todos os procedimentos encontram-se documentados nos papéis de trabalho da auditoria, e a metodologia adotada é detalhada a seguir.

1.5.1. Estudo Preliminar

O estudo preliminar compreendeu a análise da auditoria realizada pelo Tribunal de Contas da União, o exame da legislação aplicável, a identificação das medidas implementadas e o conhecimento da estrutura de governança em proteção de dados do TRT4. Com base na matriz de planejamento elaborada pelo TCU, a equipe promoveu adaptações para adequá-la ao contexto do TRT4. A partir da estrutura originalmente adotada pelo Tribunal de Contas, composta por dois eixos e nove dimensões, foram definidas duas questões e onze subquestões de auditoria, que serviram de referência para a condução dos trabalhos.

1.5.2. Programa de Auditoria

Após o levantamento preliminar, a equipe responsável pelo trabalho elaborou o Programa de Auditoria, que apresentou os critérios aplicáveis, o objetivo geral, as questões de auditoria e o detalhamento dos procedimentos e dos testes a serem aplicados na fase de execução, bem como a estimativa de custos, os recursos humanos necessários e o cronograma previsto. O Programa foi compartilhado com a unidade auditada para ciência sobre as diretrizes e os critérios legais que embasam a execução da auditoria (documento nº 8).

Na sequência, foi realizada reunião de abertura da auditoria com representantes do Subcomitê de Proteção de Dados Pessoais e da Diretoria-Geral (Unidade de Apoio Executivo), em 24.03.2026, com o intuito de apresentar as principais informações sobre a auditoria e esclarecer alguns pontos sobre o objeto (documentos nºs 11 e 12). Na ocasião, foi oportunizada à área auditada a inclusão de algum item no escopo do trabalho, conforme preconizado no parágrafo único artigo 9º da Portaria GP.TRT4 nº 3.215/2024.

Tendo em vista que não houve manifestação das unidades envolvidas acerca da alteração do escopo, foi consolidado o Programa de Auditoria.

1.5.3. Coleta de Dados

Para a coleta dos dados necessários ao alcance do objetivo do trabalho, a equipe analisou os documentos compartilhados pela área auditada. Também foram coletadas informações presentes em instrumentos contratuais formalizados pelo TRT4 em 2025 e início de 2026, mediante consulta ao sistema SILC. Além disso, foram extraídos dados referentes à capacitação de magistrados(as) e servidores(as) do sistema PAS.

1.5.4. Análise

Na sequência, a equipe reuniu e examinou todas as informações coletadas sob a perspectiva das questões de auditoria e dos critérios adotados como referência para o presente trabalho. Concluída a fase de execução, foi realizada, em 19.06.2026, reunião com o Encarregado de Dados Pessoais e representantes da Diretoria-Geral – Unidade de Apoio Executivo do Subcomitê, para apresentação e discussão das conclusões preliminares da equipe de auditoria em relação a cada subquestão avaliada (documento nº 20).

1.5.5. Elaboração da Matriz de Achados e do Relatório Preliminar

Com base nos resultados obtidos, a equipe de auditoria elaborou a Matriz de Achados, que reuniu as informações relacionadas aos achados de auditoria e às eventuais oportunidades de melhoria. Após aprovação da supervisora, foram consolidados os achados que compõem o presente relatório.

A equipe designada realizou uma reunião para apresentar os achados à unidade auditada, em 26.06.2026 (documentos nºs 22 e 23), a fim de promover o diálogo sobre as constatações do trabalho, as possíveis soluções para os problemas identificados e as propostas de encaminhamento preliminares. Após a reunião, foi encaminhado o Relatório Preliminar com a consolidação dessas informações à unidade auditada.

1.5.6. Manifestação da área responsável

O relatório preliminar foi submetido à manifestação da Diretoria-Geral, enquanto Unidade de Apoio Executivo do Subcomitê, oportunidade em que foram apresentados esclarecimentos adicionais sobre atos e fatos administrativos sob a responsabilidade do colegiado.

1.5.7. Elaboração do Relatório Final

Por fim, recebidas e analisadas as manifestações, foram consolidadas as propostas de encaminhamento da equipe de auditoria no presente relatório.

1.6. CRITÉRIOS DE AUDITORIA

Todos os critérios considerados para este trabalho foram apresentados no Programa de Auditoria (documento nº 8), dos quais se destacam os seguintes:

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução CNJ nº 363/2021 - Estabelece medidas para o processo de adequação à LGPD a serem adotadas pelos tribunais;
- Resolução CSJT nº 309/2021 - Estabelece diretrizes e orientações para a formulação de Políticas de Privacidade e Proteção de Dados Pessoais no âmbito dos Tribunais Regionais do Trabalho;
- Portaria GP.TRT4 nº 2.036/2021 - Institui a Política de Privacidade e Proteção de Dados Pessoais no âmbito do Tribunal Regional do Trabalho da 4ª Região;
- Instrução Normativa GSI/PR nº 5/2021 - Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;
- ABNT NBR ISO/IEC 27002:2022 – Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação.

1.7. BENEFÍCIOS ESTIMADOS

Entre os benefícios estimados desta auditoria estão: (i) o fortalecimento da governança institucional e da cultura de privacidade e de proteção de dados pessoais, por meio de ações de conscientização e de capacitação voltadas a magistrados(as) e servidores(as); (ii) o aprimoramento do nível de conformidade do TRT4 com a LGPD, com a continuidade da elaboração dos Inventários de Dados Pessoais, a melhoria da qualidade das informações neles registradas e a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais para operações de maior risco; e (iii) a implementação e o aperfeiçoamento de controles relacionados ao compartilhamento de dados com terceiros e ao uso de serviços de computação em nuvem.

2. RESULTADOS DE AUDITORIA

Este capítulo apresenta os resultados da auditoria, obtidos por meio de procedimentos destinados a responder às duas questões deste trabalho. De modo geral, o TRT4 vem implementando medidas de adequação à LGPD alinhadas à legislação vigente. Destaca-se o empenho da Assessoria de Otimização de Processos, vinculada à Diretoria-Geral (Unidade de Apoio Executivo ao Subcomitê de Proteção de Dados Pessoais), e do Encarregado pelo Tratamento de Dados Pessoais do Tribunal, evidenciando o compromisso institucional com a adoção dessas medidas.

O Apêndice A apresenta as respostas detalhadas da Secretaria de Auditoria para cada procedimento avaliado no presente trabalho. Conforme exposto, alguns procedimentos testados apresentaram resultado negativo; entretanto, a equipe de auditoria optou por não propor recomendações específicas para esses pontos. Tal decisão considerou: (i) a capacidade operacional da força de trabalho da instituição; (ii) o contexto normativo e as exigências das resoluções dos Conselhos Superiores, bem como o fato de a norma do CSJT estar em processo de revisão; (iii) as medidas já iniciadas pela Administração e a elaboração do Plano de Ação para 2026 (em andamento); e (iv) o potencial de contribuição para o aprimoramento da proteção de

dados pessoais no Tribunal, tratando-se da primeira auditoria da Seaudi nessa temática. Assim, das 11 subquestões previstas, cinco geraram propostas de encaminhamento.

Nesse contexto, e considerando o papel da auditoria interna de agregar valor e contribuir para o aprimoramento da gestão, apresentam-se, a seguir, quatro achados de auditoria.

A1. O aumento da participação em ações de conscientização e capacitação sobre proteção de dados pessoais, adequadas aos diferentes níveis de responsabilidade e atribuições dos(as) magistrados(as) e servidores(as), contribuirá para a melhoria das atividades de tratamento de dados pessoais no TRT4.

Situação encontrada

Conforme destacam Teixeira e Guerreiro (2022, p. 175)[9], a legislação de proteção de dados tem como propósito não apenas resguardar os interesses dos titulares, mas também promover a conscientização dos agentes de tratamento – controladores e operadores – de que as atividades de tratamento envolvem direitos fundamentais dos cidadãos. Isso é evidenciado pelas boas práticas elencadas na LGPD, a exemplo do artigo 50:

> **Os controladores e operadores, no âmbito de suas competências**, pelo tratamento de dados pessoais, individualmente ou por meio de associações, **poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização**, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, **as ações educativas**, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (grifo nosso)

Alinhada à LGPD, a Resolução CNJ nº 363/2021 também trata do tema da capacitação:

> Art. 1º **Estabelecer medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) a serem adotadas pelos tribunais do país (primeira e segunda instâncias e Cortes Superiores), à exceção do Supremo Tribunal Federal, para facilitar o processo de implementação no âmbito do sistema judicial, consistentes em**:
> I – criar o Comitê Gestor de Proteção de Dados Pessoais (CGPD), que será o responsável pelo processo de implementação da Lei nº 13.709/2018 em cada tribunal, com as seguintes características:

[9] TEIXEIRA, Tarcisio; GUERREIRO, Ruth Maria. Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo – 4ª edição. São Paulo: SaraivaJur, 2022.

> a) a composição do referido Comitê deverá ter caráter multidisciplinar e ter em vista o porte de cada tribunal;
> b) **caberá a cada tribunal a decisão de promover a capacitação dos membros do CGPD sobre a LGPD e normas afins, o que poderá ser viabilizado pelas academias ou escolas judiciais das respectivas Cortes de Justiça**; [...]
> IX – **organizar programa de conscientização sobre a LGPD, destinado a magistrados, a servidores, a trabalhadores terceirizados, a estagiários e residentes judiciais, das áreas administrativas e judiciais de primeira e segunda instâncias** e Cortes Superiores, à exceção do Supremo Tribunal Federal; (grifo nosso)

Além disso, durante o 1º Encontro Nacional de Encarregadas e Encarregados do Poder Judiciário, realizado em outubro de 2025, foi apresentada a Carta de Brasília, consolidando as reflexões apresentadas ao longo do evento. Nesse documento também são apresentadas boas práticas referentes à capacitação dos(as) Encarregados(as) de Dados Pessoais, magistrados(as), servidores(as), terceirizados(as) e estagiários(as):

> **1. O fortalecimento do papel institucional do Encarregado**
> [...] Importante ressaltar que o exercício da função de Encarregada e de Encarregado pelo Tratamento de Dados Pessoais, pela sua tecnicidade, **pressupõe capacitação específica** ou experiência reconhecida, assegurada política permanente de formação pelas Escolas Judiciais e parceiros externos, com atualizações periódicas, sem exigir formação profissional ou certificação determinada, nos termos do art. 14 da Resolução CD/ANPD nº 18/2024.
> [...]
> **5. A consolidação da cultura de privacidade e proteção de dados pessoais**
> A consolidação de uma cultura de privacidade e proteção de dados pessoais **exige programas permanentes de formação e sensibilização, envolvendo magistrados, servidores, colaboradores terceirizados e estagiários, com ênfase também em segurança da informação e no uso ético da inteligência artificial**. **Sublinhamos a importância de que os tribunais instituam política permanente de formação com dotação orçamentária, metas e cronograma anual, abrangendo LGPD**, segurança da informação, gestão de incidentes, prova digital e inteligência artificial responsável, em cooperação com o ANPD, instituições acadêmicas e outros atores do sistema de Justiça, de modo a fomentar a cultura de proteção de dados, consolidar capacidades institucionais e reduzir riscos de conformidade. (grifo nosso)

Carloto (2023, p. 254)[10], ao tratar das etapas para implementação da LGPD na prática em uma organização, reflete sobre a importância da elaboração de plano de treinamento:

> Deverá ser criado um plano de treinamento em privacidade com **palestras e treinamentos completos para os membros do comitê e pessoas chave na rede de privacidade da entidade, além de treinamentos constantes,**

[10] CARLOTO, Selma. Lei geral de proteção de dados: incluindo modelos, segurança da informação e fases de implantação. – 4ª edição. São Paulo: LTr, 2023.

> **ainda que mais básicos, para todos os empregados**, sempre que for necessário, **além de treinamentos de segurança da informação** sobre as políticas de segurança da informação. (grifo nosso)

No âmbito deste TRT4, destaca-se o empenho da Escola Judicial do TRT4 em capacitar magistrados(as), servidores(as), estagiários(as) e o público externo, promovendo treinamentos anuais sobre o tema LGPD. Cita-se a elaboração do Plano de Capacitação: 2025 que contempla, para o tópico referente à formação administrativa, um eixo temático relacionado à comunicação e transparência. Conforme detalhado nesse Plano, um dos subeixos diz respeito à Transparência e Proteção de Dados (BRASIL, 2025, p. 38)[11]:

> 4.2.6 Comunicação e Transparência
> Reúne as **competências necessárias ao reconhecimento de normas legais que regem a proteção de dados pessoais, aplicando-as ao caso concreto**; bem como a identificação de comunicação interna e externa e relacionamento com a mídia; reconhecer normas de protocolo, cerimonial e representação em eventos.
> [...]
> O eixo Comunicação e Transparência engloba os seguintes subeixos:
> - **Transparência e Proteção de Dados**
> - Comunicação Interna e Externa e Relacionamento Institucional
> - Comunicação, Linguagem e Redação (grifo nosso)

Adicionalmente, em análise à página da Escola Judicial do TRT4, verificou-se que, nos últimos anos, foram ofertados cursos relacionados à proteção de dados destinados ao público interno e externo, conforme elencado no Quadro 2:

Quadro 2 – Cursos sobre proteção de dados pessoais oferecidos pela Ejud4

Ano	Curso na temática proteção de dados pessoais
2021	• Curso de Formação Continuada (CFC) sobre a Lei Geral de Proteção de Dados e suas Repercussões na Justiça do Trabalho e nas Relações Laborais (Enamat), realizado nos dias 18.03 e 19.03, • Seminário LGPD e Fluxo de Dados no Processo Judicial (parceria com ESA/OAB-RS / Apoio: ASRDT), na modalidade telepresencial, realizado nos dias 15.04 e 16.04, • Curso Lei Geral de Proteção de Dados – LGPD, na modalidade EaD autoinstrucional, realizado nos dias 04.05 a 31.05, • Curso LGPD para Áreas Administrativas: Atualização em Proteção de Dados – Teoria e Prática – T1/2021, na modalidade EaD autoinstrucional, realizado nos dias 04.05 a 31.05, • Programa Atualização Normativa e Jurisprudencial – Lei Geral de Proteção de Dados, na modalidade telepresencial, realizado no dia 23.08,

[11] BRASIL. Tribunal Regional do Trabalho (Região, 4ª). Escola Judicial do TRT4. Plano de capacitação [recurso eletrônico] / Escola Judicial do Tribunal Regional do Trabalho da 4ª Região; Organização e texto: Camila Frigo, Lara Gobhardt Martins Fortes. Porto Alegre: Ejud4, 2025.

	• CFC sobre Lei Geral de Proteção de Dados e seus Impactos nas Relações de Trabalho, na modalidade EaD, realizado nos dias 18.10 a 01.12.
2022	• CFC sobre Lei Geral de Proteção de Dados e seus Impactos nas Relações de Trabalho (Enamat), na modalidade EaD, realizado nos dias 28.03 a 11.05, • Programa de Atualização Normativa (6ª Encontro) – Entre o Deslumbramento e a Inovação: O Espaço das Provas Digitais no Ambiente da LGPD, na modalidade telepresencial, realizado no dia 06.04.
2023	• Curso Lei Geral de Proteção de Dados – LGPD – T1/2023, na modalidade EaD autoinstrucional, realizado nos dias 10.05 a 30.05.
2024	• Curso Introdução à Lei Geral de Proteção de Dados – LGPD – T1/2024, na modalidade EaD autoinstrucional, realizado nos dias 04.04 a 30.04.
2025	• Curso Introdução à Lei Geral de Proteção de Dados – LGPD – T1/2025, na modalidade EaD autoinstrucional, realizado nos dias 10.03 a 31.03, • Curso Introdução à Lei Geral de Proteção de Dados – LGPD T2/2025, na modalidade EaD autoinstrucional, realizado nos dias 03.09 a 22.09.

Dessa forma, a fim de avaliar a efetividade dessa medida, verificou-se a participação de magistrados(as) e servidores(as) do TRT4 em ações de capacitação relacionadas à LGPD. Para isso, inicialmente foram identificadas as unidades do Tribunal que realizam tratamento de dados pessoais. Segundo o Programa Institucional de Governança em Privacidade de Dados, instituído pela Portaria GP.TRT4 nº 4.948/2022, as áreas que concentram maior volume de dados pessoais são:

- Ouvidoria
- Secretaria de Apoio aos Magistrados (Seama)
- Secretaria de Auditoria (Seaudi)
- Secretaria de Comunicação Social (Secom)
- Secretaria Executiva da Escola Judicial (EJud4)
- Secretaria-Geral de Tecnologia e Inovação (SGTI)
- Diretoria-Geral (DG):
    - Secretaria de Administração (SA)
    - Secretaria de Gestão de Pessoas (Segesp)
    - Secretaria de Manutenção e Projetos (Sempro)
    - Secretaria de Orçamento e Finanças (Secof)

- Secretaria de Saúde e Assistência (SeSaúde)
- Secretaria de Serviços (SecServ)

A área auditada, em resposta à RDI Seaudi nº 3/2026 (documento nº 14), ressaltou que:

> **Questão 7.**
> [...] Por fim, cumpre salientar que, salvo melhor juízo, **todo e qualquer servidor que tenha acesso a processos administrativos físicos ou digitais, bem como a sistemas deste Regional, possui acesso a dados pessoais**. Dessa forma, não apenas as unidades acima elencadas detêm tal acesso. Ressalta-se que **tais unidades foram selecionadas** para a elaboração de IDPs com o objetivo de realizar o levantamento do tratamento de dados pessoais, **em razão de concentrarem elevado volume dessas informações, não tendo sido consideradas, à época, como as únicas unidades do Tribunal a lidar com dados pessoais**. (grifo nosso)

Assim, embora outras áreas do TRT4 também realizem operações de tratamento de dados pessoais, para os fins desta auditoria, foram consideradas apenas as unidades acima elencadas. Na análise realizada pela equipe de auditoria, foram verificados os seguintes aspectos: (i) se os respectivos **Planos Anuais de Capacitação (PAC) contemplam a avaliação do nível de conhecimento no tema proteção de dados pessoais** dos(as) servidores(as) lotados(as) nas unidades abrangidas pelo Programa Institucional de Governança em Privacidade de Dados; (ii) se **os(as) servidores(as) dessas unidades** participaram de treinamentos relacionados à proteção de dados pessoais; e (iii) se os **integrantes do Subcomitê de Proteção de Dados Pessoais** – instância interna de apoio à governança de dados pessoais do TRT4 – participaram de ações de capacitação sobre a Lei Geral de Proteção de Dados, conforme detalhado nos itens a seguir.

a) Avaliação do nível de conhecimento para a temática de proteção de dados pessoais nos Planos Anuais de Capacitação (PACs)

Na auditoria realizada para avaliar os controles implementados pelas organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (Acórdão TCU nº 1372/2025 – Plenário), o TCU ponderou que:

> 57. **É necessário que todas as pessoas da organização estejam cientes da importância dos temas privacidade e proteção de dados pessoais, bem como dos impactos e prejuízos que podem ser causados devido às violações desses dados** (e.g. sanções aplicadas pela ANPD, indenizações, danos financeiros e à imagem da instituição). [...].
> 58. Nesse sentido, é conveniente que a organização elabore um **Plano de Capacitação que contemple ações de conscientização e que determine os conhecimentos e as competências necessárias para os recursos**

> **humanos relativamente a essa temática, sobretudo no que tange aos colaboradores diretamente envolvidos em atividades que realizam o tratamento de dados pessoais**. Assim, esse **Plano de Capacitação deve mapear as lacunas de conhecimentos e de habilidades associadas ao tema e, consequentemente, planejar ações de treinamento para a sua gradual redução**.
> 59. As ações de capacitação **devem considerar diferentes níveis de envolvimento dos colaboradores no tema**, de forma que aquelas pessoas envolvidas em atividades críticas relacionadas ao tratamento de dados pessoais e que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais **recebam treinamento diferenciado, além do nível básico fornecido aos demais colaboradores**. (grifo nosso)

Dessa forma, para que os(as) servidores(as) recebam capacitação compatível com suas atribuições e responsabilidades relacionadas ao tratamento de dados pessoais, torna-se necessária a avaliação prévia do nível de conhecimento e das competências já existentes. Essa avaliação permite identificar lacunas de capacitação e direcionar as ações de treinamento de forma mais eficiente e aderente às necessidades de cada público.

O Quadro 3 apresenta a análise dos PACs das unidades abrangidas pelo Programa Institucional de Governança em Privacidade de Dados, referentes ao período 2023 a 2025, indicando se os documentos contemplam a avaliação do nível de conhecimento dos(as) servidores(as) e se há a previsão de ações de capacitação relacionadas à LGPD. Destaca-se que não foram localizados PACs para a Ouvidoria e para a Secretaria de Apoio aos Magistrados no sistema PROAD. Da mesma forma, não foram encontrados PACs da Escola Judicial e da Secretaria de Comunicação referentes aos anos de 2023 e 2024.

Quadro 3 – Avaliação dos PACs das unidades com maior volume de dados pessoais tratados

Unidade	PAC	PROAD	Avaliou o nível de conhecimento dos(as) servidores(as)	Previu alguma capacitação sobre o tema proteção de dados pessoais
Seaudi	2023	8593/2022	**Sim**	**Não**
	2024	8367/2023	**Sim**	**Não**
	2025	7003/2024	**Sim**	**Não**
Secom	2025	2265/2025 (PAC da Presidência)	**Não**	**Não**
EJud4	2025	6157/2025	**Não**	**Não**

SGTI	2023	9263/2022	**Sim**	**Sim**
	2024	8774/2023	**Sim**	**Sim**
	2025	7761/2024	**Sim**	**Sim**
DG: - SA - Segesp - Sempro - Secof - SeSaúde - SecServ	2023	652/2023	**Não**	**Não**
	2024	133/2024	**Não**	**Não**
	2025	1399/2025	**Não**	**Sim** para a Segesp

Considerando o entendimento do TCU de que as ações de capacitação devem ser planejadas com base na identificação das lacunas de conhecimentos dos(as) colaboradores(as), observa-se que **a maior parte das unidades abrangidas pelo Programa Institucional de Governança em Privacidade de Dados não possui mecanismos formais para avaliar o nível de conhecimento de seus(suas) servidores(as)**. Essa situação limita a capacidade institucional de identificar necessidades de treinamento e de planejar ações compatíveis com os diferentes níveis de responsabilidade dos(as) servidores(as) envolvidos(as) em atividades de tratamento de dados pessoais.

Pondera-se, contudo, que a ausência de previsão de ações de capacitação sobre proteção de dados pessoais nos respectivos PACs não significa, necessariamente, que os(as) servidores(as) não tenham recebido treinamento nessa temática. Conforme demonstrado na Tabela 1, servidores(as) de diversas unidades participaram de cursos sobre proteção de dados pessoais.

b) Servidores(as) treinados(as) na temática de proteção de dados

Por meio da RDI Seaudi nº 03/2026 (documento nº 13), a equipe de auditoria solicitou a relação dos(as) servidores(as) lotados(as), nos últimos três anos, nas unidades abrangidas pelo Programa Institucional de Governança em Privacidade de Dados. Adicionalmente, foi extraída do Portal de Apoio ao SIGEP-JT (PAS) uma listagem dos(as) servidores(as) que participaram de capacitações relacionadas ao tema proteção de dados pessoais no período de 2020 a 2025. A Tabela 1 apresenta a análise do cruzamento dessas informações.

Destaca-se que, para algumas unidades, observou-se que alguns(mas) servidores(as) permaneceram lotados(as) por curto período de tempo. É o caso, por exemplo, da Segesp que, em razão de sua competência para gerir a movimentação de pessoal, realiza, em determinadas situações, lotações temporárias até a definição da unidade de exercício definitiva. Por esse motivo, foram desconsiderados neste levantamento os(as) servidores(as) que permaneceram lotados(as) por período inferior a 30 dias na respectiva unidade.

Tabela 1 – Quantidade de servidores(as) capacitados em temas correlatos à LGPD lotados nas unidades com maior volume de dados pessoais tratados

Unidade	Quantidade total de servidores(as)	Servidores(as) capacitados (2020-2025)	% de servidores(as) capacitados
Ouvidoria	5	3	**60%**
Seama	12	9	**75%**
Seaudi	15	6	**40%**
Secom	16	7	**43,75%**
EJud4	41	12	**29,27%**
SGTI	149	62	**41,61%**
DG	29	16	**55,17%**
SA	51	14	**27,45%**
Segesp	108	53	**49,07%**
Sempro	51	13	**25,49%**
Secof	43	19	**44,19%**
SeSaúde	24	10	**41,67%**
SecServ	57	8	**14,04%**

Da análise da tabela acima, verifica-se que apenas três das 13 unidades avaliadas (23%) possuem mais de 50% de seus(suas) servidores(as) com pelo menos uma capacitação em temas correlatos à proteção de dados pessoais. Ou seja, **77% das unidades do TRT4 com maior volume de dados pessoais tratados possuem menos de 50% de seus(suas) servidores(as) treinados em LGPD**.

Esses resultados indicam que, embora o TRT4 disponibilize ações de capacitação sobre o tema, a participação dos(as) servidores(as) ainda se mostra limitada. Tal cenário pode comprometer a disseminação da cultura de proteção de dados e a adequada compreensão das responsabilidades relacionadas ao tratamento de dados pessoais pelas unidades que concentram maior volume dessas informações.

c) Capacitação dos(as) integrantes do Subcomitê de Proteção de Dados Pessoais

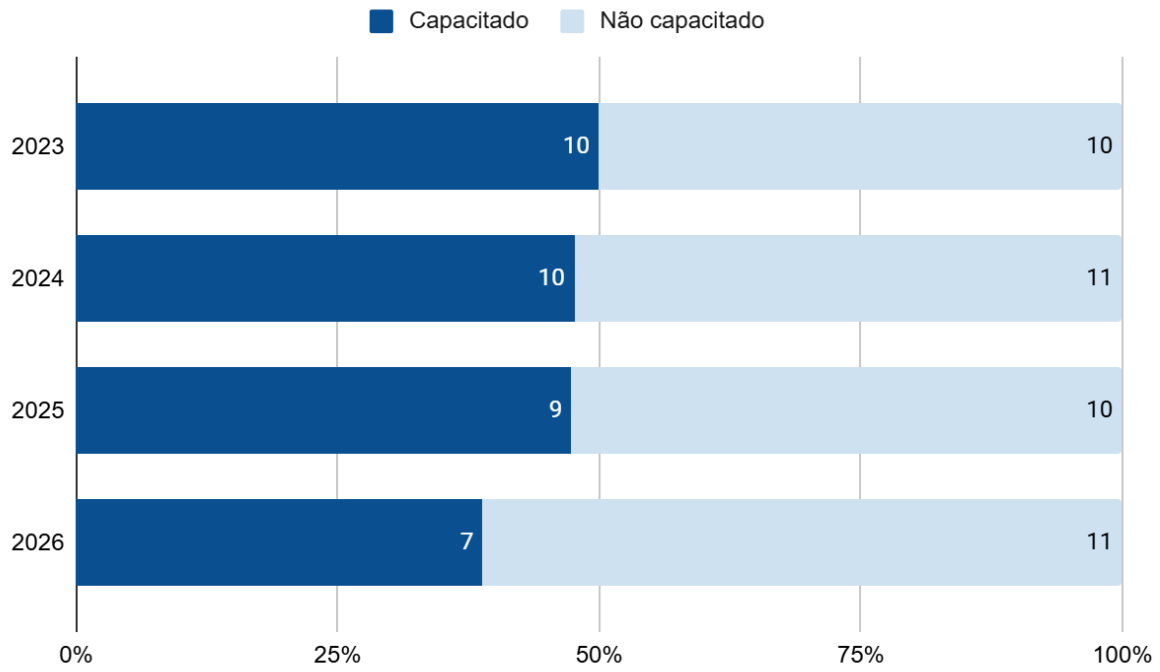
O Subcomitê de Proteção de Dados Pessoais, instituído pela Portaria GP.TRT4 nº 4.502/2022, desempenha papel relevante na estrutura de governança de proteção de dados pessoais no âmbito do TRT4. Esse colegiado, conforme artigo 2º, é composto por magistrados(as) e servidores(as) que o integram em razão do cargo ou da atribuição exercida, bem como por membros indicados pela Presidência do Tribunal ou pela Associação dos Magistrados da Justiça do Trabalho da 4ª Região. Suas competências estão definidas no artigo 3º da norma:

> Art. 3º Cabe ao Subcomitê de Proteção de Dados Pessoais:
> I – **prestar orientações e oferecer parecer técnico**, quando solicitado pelo controlador ou encarregado dos dados, **nos pedidos administrativos relacionados ao tratamento e à proteção de dados pessoais** de acordo com as diretrizes estabelecidas na LGPD, nas normas do CNJ, TST e CSJT e internas do Tribunal;
> II – **avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade do Tribunal Regional do Trabalho da 4ª Região com as disposições da LGPD**, e com as normas do CNJ, TST e CSJT e internas do Tribunal; e
> III – **auxiliar o controlador de dados quando solicitado**, na formulação de princípios e diretrizes para a gestão de dados pessoais e na sua regulamentação.
> Parágrafo único. A Ouvidoria do Tribunal é a unidade responsável pelo recebimento das demandas relacionadas à LGPD. (grifo nosso)

Para os(as) integrantes do Subcomitê de Proteção de Dados Pessoais, foi realizada avaliação similar à descrita no item anterior. Inicialmente, a equipe de auditoria identificou os(as) magistrados(as) e servidores(as) que integraram o Subcomitê nos últimos três anos (2023 a 2025) e sua composição atual (em 12.06.2026). Em seguida, essas informações foram cruzadas com os dados do relatório extraído do Portal de Apoio ao SIGEP-JT (PAS), mencionado no item “b”, contendo os registros de capacitação relacionados à temática de proteção de dados

pessoais. Com base nesse cruzamento, a equipe de auditoria elaborou o gráfico a seguir.

Gráfico 1 – Quantitativo de integrantes do Subcomitê de Proteção de Dados Pessoais com capacitação em proteção de dados ao longos dos últimos anos



Pela análise do gráfico, observa-se que houve uma redução no quantitativo de integrantes do Subcomitê capacitados em proteção de dados pessoais ao longo dos anos. **Em 2023, 50% dos(as) integrantes do Subcomitê possuíam capacitação na temática. Em 2024 e 2025, esse percentual foi de aproximadamente 47%. Já na composição atual, o índice é de cerca de 39%.** Contudo, deve-se considerar que a atual composição do colegiado foi constituída nos últimos seis meses, sendo razoável supor que esse percentual aumente à medida que seus(suas) integrantes participem de novas ações de capacitação.

Considerando as atribuições do Subcomitê de Proteção de Dados Pessoais relacionadas à orientação, avaliação e proposição de medidas voltadas à conformidade do Tribunal com a LGPD, é fundamental que seus(suas) integrantes possuam conhecimentos atualizados sobre proteção de dados pessoais. A capacitação contínua dos membros do colegiado contribui para o adequado exercício de suas competências e para o fortalecimento da governança de dados pessoais no TRT4.

Critérios de auditoria

- Lei nº 13.709/2018, artigo 50;
- Resolução CNJ nº 363/2021, artigo 1º;
- Acórdão TCU nº 1.372/2025 – Plenário (itens 57 a 59 do Relatório).

Evidências

- Portaria GP.TRT4 nº 4.502/2022;
- RDI Seaudi nº 03/2026;
- Portal da Escola Judicial do TRT da 4ª Região;
- Portal de Apoio ao SIGEP-JT (PAS);
- PROADs nºs 8593/2022, 9263/2022, 652/2023, 8367/2023, 8774/2023, 133/2024, 7003/2024, 7761/2024, 1399/2025, 2265/2025, 6157/2025.

Possíveis causas

- Grau de maturidade em governança e gestão de riscos de privacidade e proteção de dados em processo de amadurecimento no TRT4;
- Programa Institucional de Gestão de Pessoas por Competências em estágio inicial de implementação, dificultando a identificação sistemática das competências e necessidades de capacitação relacionadas à proteção de dados pessoais;
- Sobrecarga de trabalho das áreas administrativas que concentram o maior volume de dados pessoais tratados pelo Tribunal, reduzindo a disponibilidade dos(as) servidores(as) para participação em ações de capacitação;
- Rotatividade de servidores(as) nas unidades que concentram maior volume de tratamento de dados pessoais;
- Alterações na composição do Subcomitê de Proteção de Dados Pessoais, em decorrência de mudanças de gestão, movimentação de pessoal ou motivos particulares de seus(suas) integrantes.

Efeitos

- Limitação da capacidade institucional de identificar necessidades de treinamento e de planejar ações compatíveis com os diferentes níveis de responsabilidade dos(as) servidores(as) que tratam dados pessoais;

- Baixa disseminação da cultura de proteção de dados e compreensão insuficiente das responsabilidades relacionadas ao tratamento de dados pessoais pelas unidades do TRT4;
- Maior probabilidade de descumprimento de obrigações previstas na LGPD e nos normativos relacionados à proteção de dados pessoais;
- Possibilidade de ocorrência de prejuízos ao Tribunal decorrentes de violações de dados pessoais, como sanções aplicadas pela ANPD, condenações judiciais para pagamento de indenizações e danos à imagem.

Manifestação do Auditado

Em sua manifestação, a DG informou que (documento nº 27):

> A ação institucional mais recente voltada à conscientização e à capacitação em proteção de dados pessoais foi realizada em 28 de maio de 2026, por meio da publicação de matéria no portal Vox, divulgando o curso "Introdução à Lei Geral de Proteção de Dados (LGPD)", promovido pela Escola Judicial. **A iniciativa teve como objetivo incentivar a participação de magistrados(as), servidores(as) e estagiários(as), reforçando a importância da capacitação contínua como instrumento de fortalecimento da governança em proteção de dados no âmbito do Tribunal**.
> Além da divulgação do curso, a matéria apresentou conceitos fundamentais da Lei Geral de Proteção de Dados, abordando princípios como finalidade, adequação, necessidade, segurança no tratamento de dados pessoais e boas práticas relacionadas à privacidade, contribuindo para a disseminação da cultura de proteção de dados no TRT da 4ª Região.
> **Em consulta realizada à Escola Judicial, foi informado que a referida capacitação contou com 72 inscritos, demonstrando interesse e engajamento do público interno na temática**.
> Está prevista a abertura de nova turma do mesmo curso em agosto de 2026. Na ocasião, **será promovida nova campanha institucional de divulgação e mobilização, com especial direcionamento aos integrantes do Subcomitê de Proteção de Dados Pessoais que ainda não participaram da capacitação, bem como aos magistrados e servidores que atuam em processos e atividades que envolvam o tratamento de dados pessoais sensíveis ou de maior risco à privacidade**.
> **O Plano de Ação em LGPD para o biênio 2026–2027 contemplará novas iniciativas de conscientização e capacitação, com o objetivo de ampliar o alcance das ações educativas, promover a atualização permanente dos agentes públicos e consolidar, de forma progressiva, a cultura institucional de proteção de dados pessoais no TRT da 4ª Região**. (grifo nosso)

Conclusão da Equipe de Auditoria

A Diretoria-Geral, na qualidade de Unidade de Apoio Executivo do Subcomitê de Proteção de Dados Pessoais, não apresentou discordância em relação à situação encontrada neste achado. A unidade apresentou evidências das providências que

estão sendo adotadas para ampliar o nível de conscientização e de capacitação de magistrados(as) e servidores(as) em temas relacionados à LGPD.

Diante do exposto, esta equipe de auditoria entende pertinente manter a proposta de encaminhamento formulada para o achado A1. A proposta tem por objetivo monitorar a continuidade das ações de conscientização e capacitação em proteção de dados pessoais, contribuindo para a disseminação da cultura de privacidade, o adequado exercício das responsabilidades relacionadas ao tratamento de dados pessoais e o aprimoramento da governança desses dados no TRT4.

Proposta de Encaminhamento

R1. RECOMENDA-SE ao Tribunal Regional do Trabalho da 4ª Região que, a fim de mitigar o risco de descumprimento das obrigações previstas na legislação e de prejuízos decorrentes de violações de dados pessoais, promova ações de conscientização e de capacitação em proteção de dados pessoais, especialmente para magistrados(as) e servidores(as) que desempenham atividades críticas relacionadas ao tratamento de dados pessoais, considerando os diferentes níveis de responsabilidade e atribuições exercidas, de forma a atender ao disposto na Lei nº 13.709/2018 e na Resolução CNJ nº 363/2021.

A2. A continuidade da elaboração dos Inventários de Dados Pessoais e o aprimoramento da qualidade das informações neles registradas contribuirão para o fortalecimento da governança em proteção de dados pessoais e para a conformidade do TRT4 com a LGPD.

Situação encontrada

A LGPD, estabelece, em seu artigo 37 que:

> Art. 37. O controlador e o operador devem manter **registro das operações de tratamento de dados pessoais que realizarem**, especialmente quando baseado no legítimo interesse. (grifo nosso)

O **Inventário de Dados Pessoais** (IDP) constitui instrumento destinado a documentar e manter o registro das operações de tratamento de dados pessoais realizadas pela organização, abrangendo informações relativas à coleta, ao armazenamento, à utilização, ao compartilhamento, à retenção e à eliminação

desses dados ao longo de seu ciclo de vida. De acordo com Pinheiro (2020, p. 64)[12], o IDP constitui uma das etapas iniciais do processo de adequação à LGPD, permitindo identificar quais dados pessoais são tratados e onde se encontram. Na mesma linha, Teixeira e Guerreiro (2022, p. 143)[13] afirmam que: "É obrigação legal do controlador e do operador manter o registro de operações de tratamento de dados que realiza, materializando-se o princípio da prestação de contas (*accountability*)".

A importância do registro das operações de tratamento também é ressaltada por Leal e Mello (2020, p. 135-136)[14], ao observarem que diversos princípios previstos na LGPD são concretizados por meio dessa atividade:

> **Diversos princípios da LGPD são verificados nessa atividade de registro das operações**, tais como o **princípio da finalidade** (a operação deve ter um propósito legítimo), **da adequação** (o tratamento deve ser compatível com a finalidade, ou seja, sem extrapolar seu propósito), **da necessidade** (deve-se operar o mínimo necessário para atingir a finalidade), **da transparência** (garantir informações claras ao titulares dos dados pessoais), **da segurança** (busca garantir que as melhores medidas técnicas e administrativas serão utilizadas para proteger os dados pessoais) e o **da responsabilização** (os agentes de tratamento podem ser responsabilizados individualmente pela violação da LGPD).
> Nesse ponto, faz-se oportuno esclarecer que a previsão da criação de um "inventário" dos dados não é, em si, nova no Brasil. O Decreto de regulamentação do Marco Civil da Internet já obrigava os provedores de conexão e aplicações a manterem certos registros das suas bases de dados, ainda que o objetivo fosse voltado à segurança da informação. [...]
> A LGPD acrescenta à essa obrigação um parâmetro além da perspectiva da segurança da informação: **os agentes de tratamento de dados devem guardar registros de todas as suas operações de tratamento de dados pessoais. Ou seja, tudo o que é feito com um dado, desde a coleta até o descarte, deverá ser mantido como forma de registro**. (grifo nosso)

Nesse contexto, o inventário permite identificar e documentar, de forma estruturada, quais dados pessoais são tratados pela organização, suas finalidades, bases legais, fluxos de compartilhamento, prazos de retenção e demais aspectos relevantes do tratamento. Para que o documento cumpra adequadamente essa finalidade, é imprescindível que todas áreas que realizam tratamento de dados

---

[12] PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD) – 2ª Edição. São Paulo: Saraiva Educação, 2020.
[13] TEIXEIRA, Tarcisio; GUERREIRO, Ruth Maria. Lei Geral de Proteção de Dados: comentada artigo por artigo – 4ª Edição. São Paulo: SaraivaJur, 2022.
[14] LEAL, Ana Luisa; MELLO, Luã Maia de. Agentes de tratamento de dados pessoais. *In*: FEIGELSON, Bruno; BECKER, Daniel; CAMARINHA, Sylvia M. F. (org.). **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018** – 1ª edição. São Paulo: Thomson Reuters Brasil, 2020. p.133-142.

pessoais o elaborem, bem como que as informações nele registradas sejam completas, precisas, consistentes e atualizadas.

Com base nas disposições normativas aplicáveis e no contexto observado pela equipe de auditoria, foram identificadas duas oportunidades de aprimoramento relacionadas à ampliação da elaboração dos Inventários de Dados Pessoais no âmbito do TRT4 e à melhoria dos procedimentos de registro das operações de tratamento de dados pessoais, conforme descrito a seguir.

a) Elaboração de Inventários de Dados Pessoais

No âmbito do Poder Judiciário, a Resolução CNJ nº 363/2021, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais, dispõe que:

> Art. 2º Para o cumprimento do disposto nesta Resolução, recomenda-se que o processo de implementação da LGPD contemple, ao menos, as seguintes ações:
> I – **realização do mapeamento de todas as atividades de tratamento de dados pessoais por meio de questionário**, conforme modelo a ser elaborado pelo CNJ. (grifo nosso)

Na presente auditoria, em resposta à RDI Seaudi nº 03/2026, a área técnica informou que (documento nº 14):

> **Questão 5.**
> Antes da replicação para outras áreas do TRT4, **a elaboração inicial de IDPs relativos à processos oriundos das áreas da Diretoria-Geral teve como objetivo testar e validar a adequação do formulário elaborado, em consonância com a realidade do TRT4, com base no modelo disponibilizado pelo Governo Federal, bem como analisar a efetividade das informações arrecadadas.** Paralelamente à elaboração dos IDPs, **foi solicitada às unidades a elaboração de mapeamento dos mesmos processos**, de modo que sejam elaborados fluxogramas de cada processo, visando sua posterior otimização, inclusive por meio de eliminação de etapas desnecessárias etc.
> [...]
> **Sendo assim, o objetivo é aperfeiçoar e enriquecer o template do IDP do TRT4, fazendo uma segunda rodada dentro da área da DG e, sendo aprovado, aplicá-lo em outras áreas**.
>
> **Questão 7.**
> [..] Ressalta-se que tais unidades foram selecionadas para a elaboração de IDPs com o objetivo de realizar o levantamento do tratamento de dados pessoais, em razão de concentrarem elevado volume dessas informações, não tendo sido consideradas, à época, como as únicas unidades do Tribunal a lidar com dados pessoais.
>
> **Questão 10.**
> A unidade competente já possui **40 Inventários de Dados Pessoais preenchidos**, referentes à 40 processos de trabalho deste Tribunal (DG), aptos para subsidiar a elaboração do 1º RIPD deste TRT4 [...] (grifo nosso)

Assim, verificou-se que há iniciativas voltadas à adequação institucional à LGPD, incluindo a implementação de projeto piloto para elaboração de Inventários de Dados Pessoais e a intenção de expandir sua adoção para outras unidades que realizam tratamento de dados pessoais. Conforme demonstrado no Quadro 4, os inventários atualmente elaborados abrangem processos de trabalho de unidades vinculadas principalmente à Diretoria-Geral.

Quadro 4 – Processos de trabalho mapeados nos IDPs pelas unidades do TRT4

Unidade	Processos com Inventário de Dados Pessoais (IDP)
SA	Proc 01 – Dispensa de Licitação Proc 02 – Inexigibilidade de Licitação Proc 03 – Adesão a Registro de Preços Proc 04 – Participação em Registro de Preços Proc 05 – Seleção de fornecedor
Segesp	Segesp.0044 – Concessão de Assistência Pré-Escolar Segesp.0001 – Designação/Nomeação FC/CJ Segesp.0002 – Aposentadoria Voluntária Segesp.0006 – Marcação de férias de Juízes de 2º Grau Segesp.0011 – Nomeação para cargo efetivo
Sempro	Execução de obras de reforma Priorização de demandas de projetos Encaminhamento de projetos ao CSJT Processo de trabalho de medição de contrato de manutenção predial Aditivo contratual
Secof	Contratação de obras Relatório Mensal de Bens Imóveis Intangíveis Contratação de terceirizados Pagamento de diárias Dispensa de licitação Impacto orçamentário
Sepag	SEPAG.0001 – Inclusão de pensão alimentícia em folha de pagamento (por ordem judicial) SEPAG.0002 – Cadastramento de dados bancários para crédito da folha de pagamento SEPAG.0003 – Credenciamento de consignatárias SEPAG.0004 – Adequação de margem consignável (por ordem judicial) SEPAG.0005 – Cobrança de débitos (em decorrência de falecimento)
SeSaúde	SAÚDE-08 – Condição especial de trabalho SAÚDE-09 – Isenção de Imposto de Renda SAÚDE-10 – Cooperação técnica SAÚDE-11 – Constatação de deficiência (quando não ingressante em vaga de PCD) SAÚDE-12 – Aferição do Grau de Deficiência
SecSeg	Processo de Contratação Direta Solicitação de imagens do sistema de Circuito Fechado de Televisão

	Realização do Teste de Condicionamento Físico Registro de ocorrência de furto ou dano ao patrimônio público Solicitação de acesso ao complexo do Prédio-sede do Tribunal
SecServ	Gestão dos serviços de jardinagem Contratação de postos de trabalho para operar novo sistema de áudio/vídeo Medição do faturamento do processo de contratação de limpeza Fiscalização técnica da entrega dos materiais do contrato de limpeza Fiscalização administrativa das contratações de telefonia fixa

De acordo com o Programa Institucional de Governança em Privacidade de Dados do TRT4, a elaboração dos Inventários de Dados Pessoais deve abranger, prioritariamente, as áreas administrativas e de apoio que concentram maior volume de dados pessoais sujeitos às disposições da LGPD. Para essa finalidade, foram inicialmente previstas as seguintes unidades: Secretaria-Geral de Tecnologia e Inovação, Secretaria de Apoio aos Magistrados, Secretaria Executiva da Escola Judicial, Secretaria de Auditoria, Ouvidoria, Secretaria de Comunicação Social, Diretoria-Geral, Secretaria de Gestão de Pessoas, Secretaria de Administração, Secretaria de Orçamento e Finanças e Secretaria de Saúde e Assistência. Considerando as informações prestadas pela área auditada, observa-se que a relação de unidades prevista no Programa Institucional possui caráter inicial e exemplificativo, estando sujeita à ampliação progressiva no decorrer do processo de implementação da LGPD no âmbito do TRT4.

Não obstante os avanços observados com a realização do projeto piloto e a elaboração de cerca de 40 Inventários de Dados Pessoais referentes a processos de trabalho vinculados principalmente a unidades da Diretoria-Geral, verificou-se que **a iniciativa ainda não foi estendida a todas as unidades inicialmente contempladas pelo Programa Institucional de Governança em Privacidade de Dados**. Ademais, constatou-se que os inventários elaborados até o momento **não abrangem a totalidade dos processos de trabalho das unidades participantes do projeto piloto**.

Nesse contexto, a ampliação gradual da elaboração dos Inventários de Dados Pessoais para as demais unidades e processos de trabalho que realizam tratamento de dados pessoais poderá contribuir para o fortalecimento da governança institucional em proteção de dados pessoais, ampliando a capacidade de identificação, rastreabilidade e consolidação das informações relacionadas aos

tratamentos de dados pessoais realizados no âmbito do Tribunal. Tal iniciativa mostra-se alinhada às diretrizes de adequação institucional previstas na Resolução CNJ nº 363/2021 e ao disposto no artigo 37 da LGPD – que estabelece o dever de manutenção de registro das operações de tratamento de dados pessoais –, bem como ao princípio da responsabilização e prestação de contas previsto no artigo 6º, inciso X, da referida lei.

b) Preenchimento dos Inventários de Dados Pessoais

Na auditoria realizada para avaliar os controles implementados pelas organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (Acórdão TCU nº 1372/2025 – Plenário), o Tribunal de Contas da União aborda que o inventário de dados pessoais deve contemplar:

> 75. A organização também deve manter registro detalhado (e.g. inventário) das operações de tratamento de dados pessoais que realiza, especialmente quando baseadas no legítimo interesse (LGPD, art. 37). Esse registro pode contemplar, por exemplo: **a identificação do tratamento, sua finalidade, a base legal que o fundamenta, a descrição das categorias dos titulares de dados pessoais envolvidos, os dados pessoais coletados, o tempo de retenção dos dados, o local de armazenamento dos dados, o responsável pelo processo de tratamento e as medidas de segurança adotadas**. (grifo nosso)

A partir da análise realizada nos IDPs compartilhados com esta equipe de auditoria, observou-se que os inventários elaborados pelas unidades estão alinhados ao que recomenda o TCU. Abaixo é apresentado um quadro comparando o conteúdo recomendado pelo TCU com os campos presentes no modelo de IDP adotado pelo TRT4:

Quadro 5 – Comparativo entre o conteúdo recomendado pelo TCU para os IDPs e os campos presentes no modelo adotado pelo TRT4

Conteúdo recomendado pelo TCU	Campo do modelo de IDP adotado pelo TRT4
Identificação do tratamento	6.1 – Hipótese de Tratamento
Finalidade do tratamento	6.2 – Finalidade
Base legal que o fundamenta o tratamento	6.3 – Previsão legal
Descrição das categorias dos titulares de dados pessoais envolvidos	10 – Categorias dos titulares de dados pessoais
Dados pessoais coletados	7 – Categoria de Dados Pessoais (coluna “Descrição”) 8 – Categorias de Dados Pessoais Sensíveis (coluna “Descrição”)

Tempo de retenção dos dados	7 – Categoria de Dados Pessoais (coluna “Tempo Retenção dos Dados”) 8 – Categorias de Dados Pessoais Sensíveis (coluna “Tempo Retenção dos Dados”)
Local de armazenamento dos dados	7 – Categoria de Dados Pessoais (colunas “Fonte Retenção” e “Nome Base de Dados (Software)”) 8 – Categorias de Dados Pessoais Sensíveis (colunas “Fonte Retenção” e “Nome Base de Dados (Software)”)
Responsável pelo processo de tratamento	2 – Agentes de Tratamento e Encarregado 3 – Operador de Tratamento e Ciclo de Vida do Tratamento
Medidas de segurança adotadas	12 – Controles de Privacidade e Segurança da Informação

Todavia, nem todas as áreas que participaram do projeto piloto preencheram a integralidade dos campos listados acima. O Quadro 6 exemplifica algumas situações verificadas pela equipe de auditoria relacionadas ao correto preenchimento das informações nos inventários de dados pessoais.

Quadro 6 – Exemplos de situações com IDP incompleto

Unidade	Inventário de Dados Pessoais – Processo	Situação verificada
SA	Proc 04 – Participação em Registro de Preços	Não foi informado: ● **fonte de retenção (itens 7.2.11 e 7.14)**; ● **tempo de retenção do dado (item 7.14)**; ● **base de dados (item 7.14)**.
Segesp	Segesp.0044 – Concessão de Assistência Pré-Escolar Segesp.0001 – Designação/Nomeação FC/CJ Segesp.0002 – Aposentadoria Voluntária Segesp.0006 – Marcação de férias de Juízes de 2º Grau	Não foi informado o **tempo de retenção do dado (item 7 e item 8 para Segesp.0044 e Segesp.0002)**.
	Segesp.0011 – Nomeação para cargo efetivo	Não foi informado: ● **tempo de retenção do dado (itens 7 e 8)**; ● **fonte de retenção** e **base de dados (item 7.14)**.
Secof	Contratação de terceirizados Dispensa de licitação	Não foi informado o **tempo de retenção para alguns dados (item 7.9.4 e 7.12.3)**.

Sepag	SEPAG.0001 – Inclusão de pensão alimentícia em folha de pagamento (por ordem judicial) SEPAG.0002 – Cadastramento de dados bancários para crédito da folha de pagamento SEPAG.0003 – Credenciamento de consignatárias SEPAG.0004 – Adequação de margem consignável (por ordem judicial)	Não foi informado o **tempo de retenção do dado (item 7)**.
	SEPAG.0005 – Cobrança de débitos (em decorrência de falecimento)	Não foi informado: ● **previsão legal (item 6.3)**; ● **tempo de retenção do dado (item 7)**.
SeSaúde	SAÚDE-08 – Condição especial de trabalho SAÚDE-09 – Isenção de Imposto de Renda	Não foi informado: ● **tempo de retenção do dado (itens 7 e 8)**; ● **base de dados (itens 7 e 8)**.
	SAÚDE-10 – Cooperação técnica SAÚDE-11 – Constatação de deficiência (quando não ingressante em vaga de PCD)	Não foi informado: ● **previsão legal (item 6.3)**; ● **tempo de retenção do dado (itens 7 e 8)**; ● **base de dados (itens 7 e 8)**.
	SAÚDE-12 – Aferição do Grau de Deficiência	Não foi informado: ● **tempo de retenção do dado (itens 7 e 8)**; ● **fonte de retenção (itens 7 e 8)**; ● **base de dados (itens 7 e 8)**.
SecSeg	Solicitação de imagens do CFTV	Não foi informado: ● **tempo de retenção do dado (item 7)**; ● **base do dado (item 7)**.
	Registro de ocorrência de furto ou dano ao patrimônio público	Não foi informado a **base de dados (item 7)**.
	Solicitação de acesso ao complexo do Prédio-sede do Tribunal	Não foi informado: ● **previsão legal (item 6.3)**; ● **base de dados (item 7)**.

Adicionalmente, em relação ao **campo tempo de retenção dos dados pessoais**, destaca-se que a Política de Gestão Documental e de Gestão da Memória do TRT4, instituída pela Resolução Administrativa nº 23/2021, apresenta uma Tabela de Temporalidade e Destinação de Documentos. Conforme o Glossário, presente no Anexo I da referida norma, essa tabela constitui um “Instrumento arquivístico que determina prazos e condições de guarda e destinação final dos

documentos, com sua eliminação ou recolhimento ao arquivo permanente". Já no Anexo IV é apresentada a tabela propriamente dita, dividida em áreas meio e fim.

Da análise do IDPs, verificou-se que, em vários processos, o campo tempo de retenção não foi preenchido ou a informação diverge dos prazos estabelecidos na Tabela de Temporalidade. O Quadro 7 apresenta, de forma exemplificativa, uma comparação entre os tempos de retenção informados nos IDPs e os definidos na Tabela de Temporalidade.

Quadro 7 – Comparativo entre os tempos de retenção informados nos IDPs e os prazos definidos na Tabela de Temporalidade estabelecida pela RA TRT4 nº 23/2021

Inventário de Dados Pessoais (IDP)			Prazo conforme a Tabela de Temporalidade e Destinação de Documentos (RA nº 23/2021)
Unidade	**Processo**	**Tempo de Retenção dos Dados**	
SA	Proc 05 – Seleção de fornecedor	Indeterminado	030.2 – Cadastro de Fornecedores: ● Prazo corrente: 5 anos ● Prazo intermediário: - ● Destinação: eliminação. 030.3 Documentos cadastrais de fornecedores: ● Prazo corrente: 5 anos ● Prazo intermediário: - ● Destinação: eliminação.
Segesp	0044. Concessão de Assistência Pré-Escolar	Não informado	024.912 – Assistência Pré-escolar (creche): ● Prazo corrente: até aprovação das contas ● Prazo intermediário: 5 anos ● Destinação: eliminação.
	0001. Designação/ Nomeação FC/CJ	Não informado	023.56 – Designação, disponibilidade, redistribuição, substituição: ● Prazo corrente: 5 anos ● Prazo intermediário: 52 anos ● Destinação: eliminação.
	0011. Nomeação para cargo efetivo	Não informado	023.51 – Admissão, aproveitamento, contratação, nomeação, readmissão, readaptação, recondução, reintegração, reversão: ● Prazo corrente: 5 anos ● Prazo intermediário: 52 anos ● Destinação: eliminação.

Sempro	Aditivo Contratual	Indeterminado	004.2 – Termos de acordo, de ajustes, de contratos e de convênios e seus termos aditivos: ● Prazo corrente: enquanto vigora ● Prazo intermediário: - ● Destinação: eliminação.
Sepag	0001. Inclusão de Pensão Alimentícia em Folha de Pagamento (por ordem judicial)	Não informado	024.414 – Pensão alimentícia: ● Prazo corrente: 5 anos ● Prazo intermediário: 95 anos ● Destinação: eliminação.
	0003. Credenciamento de Consignatárias	Não informado	026.15 – Adiantamento e empréstimos a servidores: ● Prazo corrente: até quitação ● Prazo intermediário: - ● Destinação: eliminação.
SeSaúde	SAÚDE-08 – Condição especial de trabalho	Não informado	024.613 – Horário especial para teletrabalho: ● Prazo corrente: 5 anos ● Prazo intermediário: 52 anos ● Destinação: eliminação.
SecSeg	Processo de contratação direta	Indeterminado	036.1 – Requisição e contratação de serviços (inclusive licitações): ● Prazo corrente: 5 anos ● Prazo intermediário: 5 anos ● Destinação: eliminação.

À luz dessas constatações, observa-se que inconsistências no preenchimento dos Inventários de Dados Pessoais, especialmente quanto aos prazos de retenção e aos campos obrigatórios, podem comprometer a gestão do ciclo de vida dos dados pessoais, a confiabilidade dos registros e a conformidade do Tribunal com a LGPD. Nesse contexto, identifica-se oportunidade de revisão dos inventários já elaborados e de adoção de mecanismos de controle que assegurem o preenchimento, a atualização e a aderência das informações às normas institucionais e à Tabela de Temporalidade.

Critérios de auditoria

- Lei nº 13.709/2018, artigos 6º, inciso X, e 37;

- Resolução CNJ nº 363/2021, artigo 2º;
- Resolução Administrativa TRT4 nº 23/2021;
- Acórdão TCU nº 1.372/2025 – Plenário (item 75 do Relatório).

Evidências

- RDI Seaudi nº 03/2026 (documento nº 14);
- Inventários de Dados Pessoais (IDP) compartilhados com a Seaudi no projeto piloto.

Possíveis causas

- Grau de maturidade em governança e gestão de riscos de privacidade e proteção de dados em processo de amadurecimento no Tribunal;
- Sobrecarga de trabalho das áreas administrativas que concentram o maior volume de dados pessoais tratados pelo Tribunal, dificultando a priorização das atividades relacionadas à elaboração de IDPs;
- Estrutura de pessoal insuficiente para garantir a revisão independente dos IDPs preenchidos pelas áreas que tratam dados pessoais.

Efeitos

- Limitação da capacidade institucional de identificar, avaliar e mitigar os riscos associados às operações de tratamento de dados pessoais realizadas no âmbito do TRT4;
- Dificuldade de demonstrar a conformidade com o princípio da responsabilização e prestação de contas previsto na LGPD;
- Comprometimento da rastreabilidade, consistência e comparabilidade das informações registradas nos Inventários de Dados Pessoais;
- Risco de retenção, armazenamento e eliminação de dados pessoais por período superior ou inferior ao necessário para atendimento das finalidades institucionais e requisitos legais aplicáveis.

Manifestação do Auditado

Em sua manifestação, quanto ao item “a” da situação encontrada, a DG informou que (documento nº 27):

> **Faz parte do escopo do Plano de Ação da Lei Geral de Proteção de Dados (LGPD) para o biênio 2026–2027 a conclusão da análise e da**

> **avaliação dos Inventários de Dados Pessoais (IDPs) existentes**, com vistas à finalização do primeiro Relatório de Impacto à Proteção de Dados Pessoais (RIPD) do Tribunal Regional do Trabalho da 4ª Região (TRT4).
> Concluída essa etapa, será realizada uma avaliação da adequação do modelo atualmente adotado para os IDPs, a fim de verificar se sua estrutura fornece informações suficientes para subsidiar a elaboração de RIPDs efetivos, capazes de identificar riscos relevantes, produzir diagnósticos consistentes e orientar a implementação de medidas de tratamento e melhoria dos processos relacionados à proteção de dados pessoais.
> **Caso o modelo seja considerado adequado, os Inventários de Dados Pessoais passarão a ser utilizados de forma contínua e institucionalizada, sendo disponibilizados tanto para novos processos pertencentes a áreas que já possuam IDPs elaborados quanto para processos de novas unidades do Tribunal, promovendo a expansão gradual da governança em proteção de dados e a padronização das avaliações de impacto em todo o Regional**. (grifo nosso)

Quanto ao item “b” da situação encontrada, a DG informou que (documento nº 27):

> **Informa-se que, ainda em 2026, as unidades participantes do projeto-piloto de elaboração dos Inventários de Dados Pessoais (IDPs) serão novamente convocadas para revisão dos documentos já produzidos, com o objetivo de promover a complementação, a correção e o aprimoramento das informações registradas**.
> A Diretoria-Geral prestará apoio técnico às unidades envolvidas, orientando quanto ao correto preenchimento dos Inventários de Dados Pessoais, esclarecendo dúvidas e promovendo o alinhamento necessário para assegurar maior consistência, uniformidade e confiabilidade das informações registradas.
> **No que se refere, especificamente, ao campo relativo ao prazo de retenção dos dados pessoais, as unidades serão orientadas a confrontar as informações constantes dos IDPs com a Tabela de Temporalidade prevista na Resolução TRT4 nº 23/2021**, de forma a garantir a conformidade dos registros com os normativos institucionais aplicáveis e com o disposto no art. 37 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).
> **Destaque-se, por oportuno, a existência de desafios para a execução dessa atividade. Um deles é a resistência ainda verificada por parte de alguns servidores em relação à temática da LGPD, seja por desconhecimento, seja por falta de interesse ou por ainda não compreenderem plenamente sua importância para a Instituição**.
> **Outro obstáculo verificado refere-se à disponibilidade de tempo das unidades para elaboração e revisão dos IDPs**. A atividade demanda levantamento detalhado das operações de tratamento de dados e participação ativa dos servidores, exigindo dos gestores a indicação de pessoal para essa finalidade. Em razão das demandas ordinárias das unidades, essa dedicação ocasiona sobrecarga de trabalho aos envolvidos.
> **Apesar desses desafios, o Subcomitê de Proteção de Dados Pessoais, em conjunto com a Diretoria-Geral, reafirmam seu compromisso com o aperfeiçoamento dos Inventários de Dados Pessoais e continuarão adotando medidas de orientação e apoio às unidades, buscando fortalecer a governança em proteção de dados pessoais e a conformidade com a LGPD**. (grifo nosso)

Conclusão da Equipe de Auditoria

A Diretoria-Geral, em sua manifestação, não apresentou discordância em relação à situação encontrada neste achado. A unidade apresentou medidas voltadas à continuidade, à revisão, à expansão e ao aperfeiçoamento dos Inventários de Dados Pessoais no âmbito do TRT4.

Pelo exposto, esta equipe de auditoria entende pertinente manter as duas propostas de encaminhamento formuladas para o achado A2. As propostas têm por objetivo monitorar as ações que serão adotadas para ampliar o mapeamento das operações de tratamento de dados pessoais e para aprimorar a qualidade, a consistência e a confiabilidade das informações registradas, promovendo maior conformidade do Tribunal com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com os normativos institucionais.

Proposta de Encaminhamento

R2. RECOMENDA-SE ao Tribunal Regional do Trabalho da 4ª Região que, a fim de mitigar o risco de não identificação, avaliação e tratamento dos riscos relacionados ao tratamento dos dados pessoais, bem como de comprometimento da demonstração de conformidade com a LGPD, promova a continuidade e ampliação gradual da elaboração dos Inventários de Dados Pessoais (IDP) para os processos de trabalho ainda não mapeados e para as demais unidades administrativas do Tribunal, em observância ao artigo 37 da Lei nº 13.709/2018.

R3. RECOMENDA-SE ao Tribunal Regional do Trabalho da 4ª Região que, no intuito de mitigar o risco de comprometimento da confiabilidade dos Inventários de Dados Pessoais e de conformidade com a LGPD, adote mecanismos de controle para assegurar o preenchimento adequado dos campos obrigatórios e a consistência das informações registradas, especialmente aquelas relacionadas ao prazo de retenção dos dados pessoais, com vistas a atender ao disposto no artigo 37 da Lei nº 13.709/2018 e na Tabela de Temporalidade contida na Resolução TRT4 nº 23/2021.

A3. A elaboração de Relatórios de Impacto à Proteção de Dados Pessoais para operações de maior risco contribuirá para a proteção dos direitos dos titulares de dados e para o fortalecimento da conformidade do TRT4 com a LGPD.

Situação encontrada

A LGPD, em seu artigo 5º, define o conceito de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Por sua vez, o artigo 38 estabelece que a Agência Nacional de Proteção de Dados (ANPD) poderá determinar ao controlador a elaboração desse relatório, nos termos de regulamento, além de definir o seu conteúdo mínimo.

> Art. 5º Para os fins desta Lei, considera-se:
> XVII – **relatório de impacto à proteção de dados pessoais**: 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**;
>
> Art. 38. **A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais**, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, **nos termos de regulamento**, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório **deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados**. (grifo nosso)

A doutrina especializada destaca que a elaboração do RIPD não constitui exigência aplicável a todas as atividades de tratamento de dados pessoais. Nesse sentido, Vainzof (2020, p. 147-148)[15] ressalta que:

> Conforme previsto em sua definição, **o RIPD não é obrigatório em todas as atividades de tratamento, mas somente naquelas que "pode gerar riscos às liberdades civis e aos direitos fundamentais"**, de forma que **cada organização precisa balizar a necessidade ou não de execução do RIPD, ponderando seu apetite aos riscos inerentes a cada atividade de tratamento.**
> Porém, independentemente do texto legal, com a sua finalidade de identificar vulnerabilidades e aplicar medidas e mecanismos eficazes, o RIPD é um procedimento prático de mitigação de risco ao caso concreto, indo muito além, portanto, de simplesmente atender à Lei ou ao órgão regulador. [...]
> Portanto, os riscos que geram a necessidade do RIPD são decorrentes apenas do tratamento que envolva dados pessoais e que viole a intimidade, a vida privada, a honra e a imagem das pessoas; a liberdade de expressão, de informação, de comunicação e de opinião; o livre desenvolvimento da personalidade e a dignidade das pessoas naturais; a discriminação atentatória dos direitos, para citar alguns exemplos. (grifo nosso)

[15] VAINZOF, Rony. Relatório de Impacto à Proteção de Dados Pessoais. *In*: BLUM, Renato Opice (org.). **Proteção de Dados: Desafios e Soluções na Adequação à Lei**. Rio de Janeiro: Forense, 2020. p. 141-167.

Vainzof (2020, p. 148-154)[16] destaca, ainda, que – diante da subjetividade do tema e da ausência de descrição exemplificativa ou taxativa de atividades de tratamento que motivariam a obrigatoriedade do RIPD –, poderiam ser utilizados como parâmetro os regulamentos europeu ou o britânico sobre proteção de dados. O autor apresenta exemplos de situações em que a elaboração do RIPD seria recomendável, bem como elenca alguns cenários:

> Portanto, de forma resumida, teríamos os seguintes cenários, todos pendentes de regulamentação:
>
> - **Tratamento de dados pessoais comuns**: a autoridade poderá determinar a elaboração do RIPD. Portanto, **o controlador deverá avaliar previamente as atividades que podem gerar riscos às liberdades civis e aos direitos fundamentais para decidir em quais delas será realizado o procedimento ou não**.
> - **Tratamento de dados pessoais sensíveis**: de igual forma, a autoridade poderá determinar a elaboração do RIPD. Portanto, o controlador deverá avaliar previamente as atividades que podem gerar riscos às liberdades civis e aos direitos fundamentais para decidir em quais delas será realizado o procedimento ou não, **lembrando que sempre uma atividade de tratamento que envolve dado sensível potencialmente traz maiores riscos aos titulares**.
> - **Tratamento de dados pessoais baseados em LI**: a autoridade poderá solicitar ao controlador o RIPD. Em que pese a possibilidade da interpretação de que o RIPD é obrigatório para toda e qualquer atividade baseada em LI [*Legitimate Interest,* ou Legítimo Interesse], já que, se a ANPD solicitar, subentender-se-ia que o procedimento teria que ter sido realizado no início do tratamento e não a partir da referida solicitação, não há razoabilidade para que tal entendimento prospere pelos motivos já expostos. Deverá o controlador, por boa prática, sempre realizar o LIA [*Legitimate Interest Assessment*, ou Avaliação de Legítimo Interesse] e, de acordo com a análise de riscos que possam ser gerados aos titulares, realizar ou não o DPIA [*Data Protection Impact Assessment*, ou Avaliação de Impacto à Proteção de Dados] . (grifo nosso)

A ANPD disponibiliza, em seu sítio eletrônico, guia de perguntas e respostas sobre o RIPD. Nesse documento, a agência esclarece que a elaboração desse relatório é de responsabilidade do controlador e apresenta orientações acerca de situações em que sua adoção é recomendada (BRASIL, 2022)[17]:

> **3. Em qual contexto a ANPD recomenda que seja elaborado o RIPD?**
> Como regra geral, **é recomendado elaborar o RIPD** em todo contexto em que as **operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais**

[16] VAINZOF, Rony. Relatório de Impacto à Proteção de Dados Pessoais. *In*: BLUM, Renato Opice (org.). **Proteção de Dados: Desafios e Soluções na Adequação à Lei**. Rio de Janeiro: Forense, 2020. p. 141-167.

[17] BRASIL. Agência Nacional de Proteção de Dados (ANPD). Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais. Portal ANPD, 2023. Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 16 jun. 2026.

previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados, conforme art. 5º, inciso XVII, e art. 55-J, inciso XIII, da LGPD, o que deverá ser avaliado pelo agente de tratamento.
A LGPD lista, ainda, situações específicas em que o RIPD poderá ser exigido pela ANPD, como:
· nas operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º);
· **quando o tratamento tiver como fundamento a hipótese de interesse legítimo** (art. 10, § 3º);
· **para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD** (art. 32); e
· **para controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam dados pessoais sensíveis** (art. 38)

8. O controlador deve elaborar um RIPD único para todas as suas operações de tratamento ou um RIPD para cada operação?
Um RIPD corresponde a cada projeto/processo do controlador que contenha um conjunto de operações de tratamento voltadas para uma mesma finalidade.
Em alguns casos, isso pode se traduzir em relatórios diferentes para cada operação de tratamento, especialmente se o controlador possui operações muito distintas. Ao elaborar relatórios separados para um conjunto de tratamentos que possuam a mesma finalidade, é possível visualizar melhor os tratamentos realizados e identificar com maior precisão os riscos associados a eles.
No entanto, se o controlador realiza múltiplas operações de tratamento similares em termos de natureza, finalidade e riscos é razoável que seja elaborado apenas um RIPD que inclua todas essas operações de tratamento.
É importante também observar que, em cenários em que há compartilhamento de dados pessoais entre diferentes controladores, cada controlador poderá ser responsável por um RIPD, ainda que utilizem uma plataforma compartilhada, uma vez que as finalidades do tratamento poderão ser distintas.

9. O que considerar como "alto risco" para fins de elaboração do RIPD?
Enquanto não for editado regulamento específico sobre o RIPD, os controladores podem, no que couber, **adotar como parâmetro** o conceito de tratamento de alto risco definido no art. 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela **Resolução nº 2/2022**.
De acordo com esse dispositivo, **o tratamento será de alto risco se verificada, no caso concreto, a presença de, ao menos, um critério geral ("larga escala" ou "afetar significativamente interesses e direitos fundamentais dos titulares") e de um critério específico ("uso de tecnologias emergentes ou inovadoras", "vigilância ou controle de zonas acessíveis ao público", "decisões tomadas unicamente com base em tratamento automatizado de dados pessoais" ou "utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos")**.
Considerando esses critérios, recomenda-se elaborar o RIPD, por exemplo, se o tratamento de dados pessoais abranger número significativo de titulares ("larga escala", critério geral) e dados pessoas [*sic*] sensíveis (critério específico). Outro exemplo que pode ser mencionado é a decisão tomada unicamente com base em tratamento automatizado de dados pessoais (critério específico), da qual possa resultar a negativa para o

> exercício de um direito ou para a utilização de um serviço ("afetar significativamente interesses e direitos", critério geral).
> **Ressalte-se que, para fins de elaboração do RIPD, esses critérios não devem ser considerados exaustivos, de modo que o controlador poderá verificar a existência de alto risco em situações diferentes das indicadas.** Assim, em conformidade com o princípio da responsabilização e prestação de contas, **cabe ao controlador avaliar as circunstâncias relevantes do caso concreto, a fim de identificar os riscos envolvidos e as medidas de prevenção e segurança apropriadas, considerando os possíveis impactos às liberdades e direitos fundamentais dos titulares e a probabilidade de sua ocorrência.** (grifo nosso)

Assim, observa-se que a necessidade de elaboração do RIPD não decorre da mera existência de riscos associados ao tratamento de dados pessoais, mas sim da ocorrência de situações que possam representar alto risco às liberdades civis e aos direitos fundamentais dos titulares. Nesse contexto, **cabe ao controlador avaliar as características de cada atividade de tratamento e identificar aquelas que demandam a elaboração do relatório**. Destaca-se, ainda, que a própria ANPD reconhece a inexistência, até o momento, de regulamentação específica sobre o RIPD, recomendando que os controladores utilizem como parâmetro, no que couber, o conceito de tratamento de alto risco previsto no Regulamento CD/ANPD nº 2/2022.

Conforme mencionado no achado A2, o TRT4 iniciou atividades voltadas à elaboração de Inventários de Dados Pessoais. Entretanto, até o momento da realização dos trabalhos de auditoria, nenhum RIPD havia sido elaborado. Em resposta à RDI nº 03/2026, a área auditada informou que (documento nº 14):

> **Questão 6.**
> [...] Sendo assim, o objetivo é aperfeiçoar e enriquecer o template do IDP do TRT4, fazendo uma segunda rodada dentro da área da DG e, sendo aprovado, aplicá-lo em outras áreas. **Concluída nova aplicação dentro da DG, será elaborado o RIPD**.
>
> **Questão 10.**
> **A unidade competente já possui 40 Inventários de Dados Pessoais preenchidos**, referentes à 40 processos de trabalho deste Tribunal (DG), **aptos para subsidiar a elaboração do 1º RIPD deste TRT4**. Todavia, tendo em vista a eminente atualização da Resolução CSJT n.º 309/2021, que trata das diretrizes e orientações acerca das Políticas de Privacidade e Proteção de Dados Pessoais no âmbito dos Tribunais Regionais do Trabalho, **optou-se por aguardar a publicação das alterações normativas para elaborar o RIPD já atendendo suas novas diretrizes**. (grifo nosso)

O levantamento e a documentação das operações de tratamento de dados pessoais constituem etapas relevantes para subsidiar a decisão acerca da necessidade de elaboração do RIPD. Sob essa perspectiva, verifica-se que o TRT4

se encontra em estágio inicial de implementação das práticas relacionadas à elaboração do RIPD, promovendo o levantamento dos tratamentos de dados pessoais e a consolidação de informações necessárias à avaliação dos riscos envolvidos.

Observou-se, consoante abordado no achado A2, que nem todos os processos de negócio do Tribunal possuem mapeamento completo das operações de tratamento de dados pessoais realizadas. Nesse contexto, a elaboração do RIPD pressupõe determinado grau de maturidade institucional, envolvendo o conhecimento dos processos de tratamento, a identificação dos fluxos de dados, a definição das bases legais aplicáveis e a avaliação dos riscos associados às atividades desenvolvidas pela organização.

Dessa forma, a consolidação dos Inventários de Dados Pessoais atualmente em curso no TRT4 viabilizará a identificação dos tratamentos que efetivamente possam demandar a elaboração de RIPDs, especialmente considerando que a própria LGPD e as orientações da ANPD indicam que a necessidade desse relatório está relacionada a operações de tratamento capazes de gerar alto risco aos direitos e liberdades fundamentais dos titulares de dados.

Diante desse cenário, identifica-se oportunidade de aprimoramento relacionada ao planejamento e à implementação gradual da elaboração de Relatórios de Impacto à Proteção de Dados Pessoais, com prioridade para processos de tratamento que envolvam maior volume de dados pessoais, dados pessoais sensíveis, dados de crianças e adolescentes ou que tenham potencial impacto aos direitos dos titulares.

Critérios de auditoria

- Lei nº 13.709/2018, artigos 5º, inciso XVII, e 38.

Evidências

- RDI Seaudi nº 03/2026 (documento nº 14).

Possíveis causas

- Ausência de regulamentação da Agência Nacional de Proteção de Dados acerca das hipóteses para elaboração do Relatório de Impacto à Proteção de Dados Pessoais;
- Grau de maturidade em governança e gestão de riscos de privacidade e proteção de dados em processo de amadurecimento no Tribunal;
- Sobrecarga de trabalho das áreas administrativas que concentram o maior volume de dados pessoais tratados pelo Tribunal, dificultando a priorização das atividades relacionadas à elaboração de RIPDs;
- Estrutura de pessoal insuficiente para atender às demandas de governança e proteção de dados pessoais.

Efeitos

- Limitação da capacidade institucional de identificar, avaliar e mitigar os riscos associados às operações de tratamento de dados pessoais realizadas no âmbito do TRT4;
- Dificuldade de demonstrar a conformidade com o princípio da responsabilização e prestação de contas previsto na LGPD;
- Potencial dano aos direitos e às liberdades fundamentais dos titulares de dados pessoais;
- Possibilidade de ocorrência de prejuízos ao Tribunal decorrentes de violações de dados pessoais, como sanções aplicadas pela ANPD, condenações judiciais para pagamento de indenizações e danos à imagem.

Manifestação do Auditado

Em sua manifestação, a DG informou que (documento nº 27):

> Informa-se que já **foi iniciada a elaboração da minuta do primeiro Relatório de Impacto à Proteção de Dados Pessoais (RIPD) do TRT da 4ª Região, contemplando operações de tratamento realizadas por unidades que tratam dados pessoais sensíveis e dados de crianças e adolescentes, em consonância com as prioridades estabelecidas pela Lei nº 13.709/2018**.
> A conclusão deste relatório está condicionada à revisão dos Inventários de Dados Pessoais (IDPs) que lhe servirão de base, etapa que permitirá o aprimoramento e a validação das informações necessárias à elaboração de um RIPD consistente e em conformidade com as exigências legais. Finalizada essa revisão, o relatório será concluído e disponibilizado no âmbito institucional.
> **Após a conclusão e avaliação dos resultados obtidos com esse primeiro RIPD, especialmente quanto à adequação da metodologia adotada e à qualidade das informações produzidas, será promovida a**

> **elaboração gradual de novos RIPDs, observando critérios de priorização baseados no potencial de risco das operações de tratamento, com especial atenção àquelas que envolvam elevado volume de dados pessoais, dados pessoais sensíveis e dados de crianças e adolescentes, em conformidade com os arts. 5º, inciso XVII, e 38 da Lei Geral de Proteção de Dados Pessoais**. (grifo nosso)

Conclusão da Equipe de Auditoria

A Diretoria-Geral, ao manifestar-se acerca da situação encontrada, apresentou as medidas que vêm sendo adotadas para a elaboração do primeiro Relatório de Impacto à Proteção de Dados Pessoais. Esclareceu, ainda, que, após a conclusão e a avaliação dos resultados obtidos com esse relatório, será promovida a elaboração gradual de novos RIPDs, observando critérios de priorização baseados no potencial de risco das operações de tratamento.

Dessa forma, esta equipe de auditoria entende pertinente manter a proposta de encaminhamento formulada para o achado A3. A proposta tem por objetivo fortalecer a gestão dos riscos decorrentes do tratamento de dados pessoais, promovendo a identificação, a avaliação e a mitigação dos impactos potenciais aos direitos e às liberdades fundamentais dos titulares.

Proposta de Encaminhamento

R4. RECOMENDA-SE ao Tribunal Regional do Trabalho da 4ª Região que, com vistas a mitigar riscos aos direitos e às liberdades fundamentais dos titulares de dados pessoais, promova a elaboração gradual de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) para operações de tratamento que apresentem maior potencial de impacto aos titulares, especialmente aquelas que envolvam elevado volume de dados pessoais, dados pessoais sensíveis ou dados de crianças e adolescentes, em observância ao disposto nos artigos 5º, inciso XVII, e 38 da Lei nº 13.709/2018.

A4. O gerenciamento dos riscos associados ao armazenamento de dados pessoais em serviços de nuvem e a avaliação das operações que podem caracterizar transferência internacional de dados têm o potencial de contribuir para a segurança e a proteção dos dados custodiados pelo TRT4.

Situação encontrada

A LGPD, em seu artigo 5º, conceitua o tratamento, a transferência internacional de dados e o uso compartilhado de dados nos seguintes termos:

> Art. 5º Para os fins desta Lei, considera-se:
> X – **tratamento**: **toda operação realizada com dados pessoais**, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, **armazenamento**, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XV – **transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI – **uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; (grifo nosso)

Toda organização que compartilhe dados pessoais com terceiros deve identificar, avaliar e tratar os riscos associados ao tratamento, adotando controles adequados para garantir a conformidade com a legislação vigente e a proteção dos direitos dos titulares dos dados pessoais. Nos casos de **tratamento de dados pessoais em soluções de computação em nuvem**, a Instrução Normativa GSI/PR nº 5/2021, aplicável aos órgãos e entidades da Administração Pública Federal, constitui importante referência de boas práticas para assegurar a confidencialidade, a integridade e a disponibilidade das informações tratadas e compartilhadas pelo Poder Público.

Quando o compartilhamento de dados configurar uma **transferência internacional de dados** – seja para empresas sediadas no exterior ou que utilizem servidores localizados fora do país –, devem ser observados os requisitos estabelecidos nos artigos 33 a 36 da LGPD, assegurando-se que o país de destino ou as cláusulas contratuais proporcione grau de proteção compatível com aquele exigido pela legislação brasileira.

Considerando o contexto observado durante esta auditoria, foram identificadas duas oportunidades de aprimoramento relacionadas aos procedimentos de tratamento de dados pessoais em solução de computação em nuvem e à possível transferência internacional de dados pessoais, conforme descrito nos itens a seguir.

a) Tratamento de dados pessoais em solução de computação em nuvem

A Instrução Normativa GSI/PR nº 5/2021 estabelece requisitos mínimos para adoção segura de soluções em nuvem pelos órgãos da Administração Pública Federal, com o objetivo de elevar o nível de proteção das informações tratadas com o uso dessa tecnologia. Essa norma prevê requisitos que devem ser observados antes da transferência de serviços ou informações para provedores de computação em nuvem, incluindo a conformidade com a legislação brasileira, a realização de gerenciamento de riscos e a avaliação da classificação da informação para definição de quais informações podem ser armazenadas em nuvem:

> Art. 11. Antes de transferir serviços ou informações para um provedor de serviço de nuvem, os órgãos ou as entidades deverão, no mínimo:
> I – **garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros as seguintes operações**:
> a) de coleta, **armazenamento**, guarda e tratamento de registros de dados pessoais; e
> b) de comunicações realizada por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional;
> II – **realizar o gerenciamento de riscos**, precedido por análise e **relatório de impacto de dados pessoais**, em conformidade com a legislação, dos seguintes itens:
> a) **o tipo de informação a ser migrada**;
> b) o fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;
> c) o valor dos ativos envolvidos; e
> d) os benefícios da adoção de uma solução de computação em nuvem, em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro;
> [...]
> V – **avaliar quais informações serão hospedadas na nuvem**, considerando:
> a) **o processo de classificação da informação de acordo com a legislação**;
> b) o valor do ativo de informação;
> c) os controles de acessos físico e lógico relativos à segurança da informação; e
> d) o modelo de serviço e de implementação de computação em nuvem;
> [...]
> Art. 17. **Em relação ao tratamento da informação em ambiente de computação em nuvem**, o órgão ou a entidade, **além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais**, **deve observar as seguintes diretrizes**:
> I – **informação sem restrição de acesso** poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;
> II – **informação classificada em grau de sigilo** e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e

> III – poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:
>
> a) **a informação com restrição de acesso** prevista na legislação, conforme o Anexo a esta Instrução Normativa;
>
> b) o **material de acesso restrito** regulado pelo próprio órgão ou pela entidade;
>
> c) a **informação pessoal relativa à intimidade, vida privada, honra e imagem**; e
>
> d) o documento preparatório não previsto no inciso II do caput. (grifo nosso)

Na mesma linha, a norma ABNT NBR ISO/IEC 27002:2022, que estabelece diretrizes para controles de segurança da informação, prevê a necessidade de gerenciamento dos riscos decorrentes da utilização de serviços prestados por terceiros. Em seu item 5.19, a norma orienta que as organizações estabeleçam processos e controles apropriados para proteger os ativos, incluindo provedores de serviços em nuvem. Adicionalmente, o item 5.23 aborda especificamente os riscos associados à utilização de serviços em nuvem, reforçando que há controles de segurança que serão gerenciados pelo provedor de serviço e outros que são gerenciados pela organização cliente.

> **5.19 Segurança da informação nas relações com fornecedores**
>
> [...]
>
> Convém que a organização **identifique e implemente processos e procedimentos para enfrentar riscos de segurança associados ao uso de produtos e serviços prestados pelos fornecedores**. Convém que isso **também se aplique ao uso da organização de recursos de provedores de serviços em nuvem**. **Convém que esses processos e procedimentos incluam aqueles a serem implementados pela organização, bem como aqueles que a organização requer que o fornecedor implemente para o início do uso de produtos ou serviços de um fornecedor** ou para o término do uso de produtos e serviços de um fornecedor, como:
>
> [...]
>
> c) avaliar e selecionar produtos ou serviços do fornecedor que tenham controles adequados de segurança da informação e analisá-los criticamente; em particular, a precisão e a completeza dos controles implementados pelo fornecedor que **assegure a integridade do tratamento de informações** e informações do fornecedor e, consequentemente, a segurança da informação da organização;
>
> [...]
>
> f) **avaliar e gerenciar os riscos de segurança da informação associados a**:
>
> 1) **o uso das informações da organização** pelos fornecedores e outros ativos associados, incluindo riscos originário de potenciais fornecedores maliciosos;
>
> [...]
>
> m) requisitos para assegurar um término seguro do relacionamento com o fornecedor, incluindo:
>
> 1) desprovisionamento dos direitos de acesso;
>
> 2) **tratamento de informações**;
>
> 3) determinação da propriedade intelectual desenvolvida durante o engajamento;

4) portabilidade de informações em caso de alteração de fornecedor ou internalização;
5) gerenciamento de registros;
6) devolução de ativos;
7) **eliminação segura de informações** e outros ativos associados;
8) requisitos de confidencialidade em andamento;

5.23 Segurança da informação para uso de serviços em nuvem
[...]
Convém que a organização defina e comunique **como pretende gerenciar riscos de segurança da informação associados ao uso de serviços em nuvem**. [...]
O uso de serviços em nuvem pode envolver responsabilidade compartilhada pela segurança da informação e esforço colaborativo entre o provedor de serviços em nuvem e a organização que atua como cliente de serviço em nuvem. É essencial que as responsabilidades tanto para o provedor de serviços em nuvem quanto para a organização, atuando como cliente de serviço em nuvem, sejam definidas e implementadas adequadamente.
Convém que a organização defina:
[...]
d) **quais controles de segurança da informação são gerenciados pelo provedor de serviços em nuvem e quais são gerenciados pela organização como cliente de serviço em nuvem**;
e) como obter e utilizar recursos de segurança da informação fornecidos pelo provedor de serviços em nuvem;
f) como obter garantia sobre controles de segurança da informação implementados por provedores de serviços em nuvem;
Os contratos de serviços em nuvem são muitas vezes predefinidos e não estão abertos à negociação. Para todos os serviços em nuvem, convém que a organização analise criticamente os contratos de serviços em nuvem com o provedor de serviços em nuvem. Convém que um acordo de serviço em nuvem aborde os requisitos de confidencialidade, integridade, disponibilidade e manuseio de informações da organização, com objetivos apropriados de nível de serviço em nuvem e objetivos qualitativos de serviço em nuvem. **Convém que a organização também realize processos de avaliação de risco pertinentes para identificar os riscos associados ao uso do serviço em nuvem. Convém que quaisquer riscos residuais ligados ao uso do serviço em nuvem sejam claramente identificados e aceitos pela gestão apropriada da organização**. (grifo nosso)

Na auditoria realizada pelo Tribunal de Contas da União para avaliar os controles implementados pelas organizações públicas federais para adequação à LGPD, o TRT4 apresentou as seguintes informações acerca do tratamento de dados pessoais em solução de computação em nuvem:

Quadro 8 – Respostas do TRT4 ao TCU quanto ao tratamento de dados pessoais em soluções de computação em nuvem

Acerca de tratamento de dados pessoais em soluções de computação em nuvem (cloud computing), a organização:	Resposta do TRT4
Realiza o tratamento de dados pessoais em nuvem (ainda que apenas armazenamento)	**Sim**
Avaliou e pode assegurar que não há armazenamento de dados pessoais em território estrangeiro	**Não**

Realizou avaliação de riscos relativamente a esse tratamento, amparada em análise e em relatório de impacto que foram devidamente submetidos à apreciação das instâncias competentes	**Não**
Incluiu, nos instrumentos contratuais com os provedores de nuvem, cláusulas e mecanismos que instituem precauções quanto à proteção de dados	**Sim**

Fonte: Adaptado de Brasil (2025)[18]

Para a presente auditoria, em relação ao tratamento de dados pessoais em soluções de computação em nuvem e sua respectiva avaliação de riscos, a área técnica informou, em resposta à RDI Seaudi nº 03/2026, que (documento nº 14):

> **Questão 12.**
> 12.1 **Não há sistemas sensíveis operando na nuvem** e, portanto, o TRT ainda **não sentiu a necessidade de fazer essa avaliação**. Confia-se no cumprimento das cláusulas contratuais, que estabelecem a necessidade de conformidade à LGPD.
> 12.2 Considerando que não há sistemas sensíveis operando em nuvem, **tal avaliação não foi realizada**. (grifo nosso)

Entretanto, apesar da resposta de não existirem sistemas sensíveis operando na nuvem, observou-se que há o **armazenamento de dados na nuvem**. Em análise aos Inventários de Dados Pessoais compartilhados com a equipe de auditoria, verificou-se que os seguintes dados pessoais são armazenados no serviço Google Drive:

Quadro 9 – Dados Pessoais e Dados Pessoais Sensíveis armazenados do Google Drive de unidades administrativas do TRT4

Unidade	Processo	Categoria de Dados Pessoais	Descrição	Fonte de Retenção
SA	PROC 02 Inexigibilidade de Licitação	7.14.1 – Vídeo e imagem	Arquivos de vídeo, fotos digitais, links de palestras ou gravações de eventos anteriores apresentados como portfólio.	Base de dados
Segesp	SEGESP.0011	7.1.1 – Informações de identificação pessoal	Nome, endereço, telefone, e-mail pessoal	Planilha eletrônica
		7.1.2 – Informações de identificação atribuídas por	RG, CPF, Nº carteira de motorista, título de eleitor, certificado de reservista, certidão de	Planilha eletrônica

[18] BRASIL. Tribunal de Contas da União. Relatório de Feedback – Organização Tribunal Regional do Trabalho da 4ª Região. Acórdão 1.372/2025-TCU-Plenário, Relatoria Min. Walton Alencar Rodrigues. Brasília, DF: TCU, 2025. Acesso em: 16.06.2026. Disponível em: https://sites.tcu.gov.br/recursos/auditoria-sobre-lgpd/relatorios/tribunais%20do%20judiciario/TRT4.pdf.

		instituições governamentais	nascimento ou casamento, PIS/PASEP, carteira de trabalho(como forma de comprovação do PIS/PASEP)	
		7.3.1 – Detalhes pessoais	Sexo, data de nascimento, local de nascimento, estado civil, nacionalidade	Planilha eletrônica
		7.6.1 – Casamento ou forma atual de coabitação	Nome do cônjuge	Planilha eletrônica
		7.6.3 – Familiares ou membros da família	Filiação	Planilha eletrônica
		7.12.1 – Dados acadêmicos/escolares	Escolaridade, curso de graduação	Planilha eletrônica
		7.13.2 – Recrutamento	Cargo para o qual foi aprovado/classificado no concurso público	Planilha eletrônica
		Dado pessoal sensível: 8.1 – Dados que revelam origem racial ou ética	Característica étnico/racial, inscrição na lista de cotas etnico/racial	Planilha eletrônica
		Dado pessoal sensível: 8.8 – Dados referentes à saúde ou à vida sexual	PCD, tipo de deficiência, inscrição na lista de cotas PCD, sexo e identidade de gênero, dados de exames de saúde para inspeção médica admissional (exames de sangue, tipagem sanguínea)	Planilha eletrônica

Além disso, as seguintes unidades mencionaram, no campo “4.1 - Descrição do Fluxo do tratamento dos dados pessoais”, o armazenamento de dados no Google Drive:

- **Secof**: para o processo “Relatório Mensal de Bens Móveis e Intangíveis” é informado que uma das atividades é “7. Atualizar as planilhas de conciliação de saldos no Google Drive”;

- **Sempro**: para o processo de “Medição de Contratos de Manutenção Predial” é informado que os dados pessoais de trabalhadores e responsáveis técnicos (nome, CPF, endereço, telefone, salário, extratos, comprovantes, etc.) e dados cadastrais da empresa (CNPJ, endereço telefone e e-mail) são armazenados no PROAD e no Google Drive, com acesso restrito aos servidores responsáveis.

Assim, verifica-se que existem dados pessoais, inclusive sensíveis, sendo armazenados no serviço de nuvem contratado pelo Tribunal. Embora os contratos firmados com os provedores contenham cláusulas relacionadas à observância da LGPD e à proteção de dados pessoais, tais disposições não afastam a necessidade de o Tribunal realizar o gerenciamento dos riscos associados ao tratamento dessas informações. Isso porque a avaliação de riscos constitui requisito prévio à transferência de dados para provedores de serviços em nuvem, conforme previsto nas boas práticas aplicáveis.

b) Transferência internacional de dados pessoais

A Resolução CNJ nº 363/2021 estabelece, em seu artigo 1º, medidas para processo de adequação à LGPD a serem adotadas pelos tribunais do país, incluindo:

> XII – **elaborar e manter os registros de tratamentos de dados pessoais contendo informações sobre:**
> a) finalidade do tratamento;
> b) base legal;
> c) descrição dos titulares;
> d) categorias de dados;
> e) categorias de destinatários;
> f) **eventual transferência internacional**; e
> g) prazo de conservação e medidas de segurança adotadas, nos termos do art. 37 da LGPD; (grifo nosso)

O Tribunal de Contas da União também possui entendimento alinhado ao disposto no artigo 1º da Resolução CNJ nº 363/2021. Nesse sentido, conforme mencionado no item “b” do achado A2, o Acórdão TCU nº 1372/2025 – Plenário (item 75 do Relatório) ressalta a importância de as organizações manterem registros detalhados de suas operações de tratamento de dados pessoais, contemplando, entre outros aspectos, a identificação do local de armazenamento dos dados.

Consoante apresentado no quadro 8, o TRT4 respondeu **negativamente** à pergunta constante do questionário aplicado pelo TCU: “avaliou e pode assegurar que não há armazenamento de dados pessoais em território estrangeiro”. Na presente auditoria, em resposta à RDI Seaudi nº 03/2026, a área técnica informou que (documento nº 14):

> **Questão 11.**
> O TRT-4 não possui contrato de transferência de dados com empresas estrangeiras. **O TRT utiliza soluções de software como serviço (SaaS), como, por exemplo, Google Workspace, Moodle e Qualitor**. Neste sentido, os contratos estabelecidos contêm cláusulas que tratam da necessidade de conformidade à LGPD.
> Portanto, conclui-se que o contrato estabelecido atende aos requisitos estabelecidos na LGPD quanto à transferência internacional de dados.
> Como evidência, Edital de Contratação do Google.

Entretanto, nesse contexto, Carloto (2023, pág. 75)[19] pondera que:

> Foram eliminadas as fronteiras físicas na era digital e esta transferência ocorre diariamente quando as empresas utilizam e-mail, ou serviços de aplicação de internet. [...] No caso de empresas que possuem matriz no exterior e filiais no Brasil, ou mesmo **as que utilizam soluções de armazenamento em nuvem fora do país**, a transferência de dados envolve a movimentação de informações pessoais através das fronteiras internacionais. (grifo nosso)

No mesmo sentido, Chaves (2022, pág. 316)[20] exemplifica as atividades que normalmente podem envolver a transferência internacional de dados:

- compartilhamento de base de dados de RH entre empresas do mesmo grupo (matriz-filial);
- armazenamento de dados em data centers fisicamente localizados no exterior;
- terceirização de serviço de atendimento ao consumidor;
- **contratação de provedor de computação em serviço de nuvem estrangeiro**;
- **contratação de provedor de e-mail estrangeiro**.(grifo nosso)

Em relação às soluções SaaS utilizadas pelo Tribunal, foi realizada consulta à Política de Privacidade do Google Workspace. No tópico “Estrutura de transferência de dados” dessa política, vigente desde 23.08.2025, consta a seguinte informação:

> Temos servidores em todo o mundo, e suas **informações podem ser processadas em servidores localizados fora do país em que você vive**. As leis de proteção de dados variam de acordo com o país, sendo que alguns oferecem mais proteção que outros. Independentemente do local

[19] CARLOTO, Selma. Lei geral de proteção de dados: incluindo modelos, segurança da informação e fases de implementação. – 4ª Edição. São Paulo: LTr, 2023.
[20] CHAVES, Luis Fernando Prado. Da Transferência Internacional de Dados. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **LGPD: Lei Geral de Proteção de Dados comentada**. – 4ª edição revisada e atualizada. São Paulo: Thomson Reuters Brasil, 2022. p. 311-330.

> onde suas informações são processadas, aplicamos as mesmas proteções descritas na Política de Privacidade. (grifo nosso)

Assim, não foi possível identificar a localização geográfica dos servidores utilizados para armazenamento e processamento dos dados do Tribunal, tampouco concluir que tais dados permanecem integralmente armazenados em território nacional. Conforme exposto no item "a" deste achado, há armazenamento de dados pessoais, inclusive dados pessoais sensíveis, em soluções de computação em nuvem utilizadas pelo TRT4.

A respeito da transferência internacional de dados, a LGPD estabelece:

> Art. 33. A transferência internacional de dados pessoais **somente é permitida** nos seguintes casos:
> I – **para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei**;
> II – **quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de**:
> a) **cláusulas contratuais específicas para determinada transferência**;
> b) **cláusulas-padrão contratuais**;
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos; (grifo nosso)

Quanto ao inciso I, Carvalho (2020, pág. 620)[21] argumenta que:

> [...] **caberá à autoridade nacional aquilatar os elementos concretos dos ordenamentos de destino dos dados para que se verifique o grau de proteção fornecido**. Contudo, o que importa aqui assinalar é que a análise prevista pelo inciso I do art. 33 da LGPD não é pontual ou casuística, mas, sim, diz respeito à aptidão do ordenamento como um todo para garantir nível adequado de proteção de dados, de sorte que cada decisão da autoridade nacional sobre determinada jurisdição deverá ser tida como declaração de idoneidade daquele ordenamento, ao menos por certo período de tempo. Em outras palavras, **o inciso I representa uma decisão da autoridade com efeitos amplos e gerais, demonstrando o posicionamento da autoridade quanto à determinada jurisdição**. (grifo nosso)

Em consulta ao sítio da Agência Nacional de Proteção de Dados, verificou-se a publicação da Resolução CD/ANPD nº 32/2026, que reconhece a União Europeia como organismo internacional com grau de proteção adequado para fins de transferência internacional de dados. Não foram identificadas, até 29.05.2026, outras

[21] CARVALHO, Angelo Gamba Prata de. Transferência internacional de dados na Lei Geral de Proteção de Dados – Força normativa e efetividade diante do cenário transnacional. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** – 2ª edição. São Paulo: Thomson Reuters Brasil, 2020. p. 615-638.

resoluções da ANPD reconhecendo outros países ou organismos internacionais com grau de proteção adequado para essa finalidade.

Além disso, considerando os termos da Política de Privacidade do Google Workspace, não foi possível identificar os países nos quais os dados pessoais eventualmente são armazenados. Dessa forma, não há elementos suficientes para avaliar eventual enquadramento da situação na hipótese prevista no inciso I do artigo 33 da LGPD, tornando necessária a análise das demais hipóteses legais de transferência internacional de dados, especialmente aquelas previstas no inciso II do referido dispositivo.

O inciso II do artigo 33 da LGPD prevê que a transferência internacional de dados poderá ocorrer quando o controlador oferecer e comprovar garantias de observância dos princípios, dos direitos dos titulares e do regime de proteção de dados pessoais estabelecido pela Lei, por meio de mecanismos como cláusulas-padrão contratuais. O artigo 35 da LGPD atribui à Agência Nacional de Proteção de Dados a competência para definir o conteúdo das cláusulas-padrão contratuais.

> Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

Dessa forma, destaca-se que a Resolução CD/ANPD nº 19/2024 aprovou o Regulamento de Transferência Internacional de Dados e as cláusulas-padrão contratuais previstas na LGPD, conforme Anexos I e II, respectivamente. O regulamento estabelece que:

> Art. 4º **Cabe ao controlador verificar**, nos termos da Lei nº 13.709, de 14 de agosto de 2018, e deste Regulamento, **se a operação de tratamento**:
> I – **caracteriza transferência internacional de dados**;
> II – submete-se à legislação nacional de proteção de dados pessoais; e
> III – está amparada em hipótese legal e em mecanismo de transferência internacional válidos.
> § 1º **O operador prestará auxílio ao controlador mediante o fornecimento das informações de que dispuser e que se demonstrarem necessárias para o atendimento ao disposto no caput deste artigo**.
> § 2º O controlador e o operador deverão adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas, de forma compatível com o grau de risco do tratamento e com o mecanismo de transferência internacional utilizado.
> [...]

> Art. 15. **As cláusulas-padrão contratuais**, elaboradas e aprovadas pela ANPD na forma do Anexo II, **estabelecem garantias mínimas e condições válidas para a realização de transferências internacionais de dados baseadas no inciso II, alínea "b", do art. 33 da Lei nº 13.709, de 14 de agosto de 2018**.
> Parágrafo único. As cláusulas-padrão contratuais **visam garantir a adoção das salvaguardas adequadas para o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018, incluindo as determinações da ANPD**.
> Art. 16. **A validade da transferência internacional de dados, quando amparada na adoção das cláusulas-padrão, pressupõe a adoção integral e sem alteração do texto disponibilizado no Anexo II, mediante instrumento contratual firmado entre o exportador e o importador**.
> § 1º As cláusulas-padrão contratuais poderão integrar:
> I – contrato celebrado para reger especificamente transferências internacionais de dados;
> II – contrato com objeto mais amplo, inclusive mediante a assinatura de termo aditivo pelo exportador e pelo importador envolvidos na operação de transferência internacional de dados.
> § 2º As demais disposições, previstas no instrumento contratual ou em contratos coligados firmados pelas partes, não poderão excluir, modificar ou contrariar, direta ou indiretamente, o disposto nas cláusulas-padrão contratuais.
> § 3º Na hipótese do inciso II do § 1º deste artigo, as Seções I, II e III do Anexo II deverão figurar como documento anexo do instrumento contratual assinado entre exportador e importador. (grifo nosso)

Da análise do contrato da solução Google Workspace (Contrato TRT4 nº 16/2025 – PROAD nº 7676/2024), verificou-se a existência de cláusulas gerais sobre proteção de dados pessoais e de termo de responsabilidade e confidencialidade. Contudo, não foram identificadas disposições específicas acerca de eventual transferência internacional de dados que contemplem as cláusulas-padrão contratuais previstas no Anexo II da Resolução CD/ANPD nº 19/2024.

Por fim, destaca-se a auditoria que está sendo realizada pelo TCU para avaliar a confiabilidade do sistema de inteligência artificial Galileu, registrada no PROAD nº 704/2026. Em resposta a questionamento sobre a possibilidade de transferência internacional de dados decorrente do tratamento de dados pessoais pelo provedor externo de inteligência artificial, a Secretaria-Geral de Tecnologia e Inovação informou que:

> Tecnicamente, **há possibilidade de transferência internacional** para as chamadas de geração de texto. O sistema utiliza duas configurações de região:
> - **São Paulo (`southamerica-east1`)**: usado exclusivamente para geração de embeddings vetoriais, com fallback para global em caso de falha.
> - **Endpoint `global`**: usado em todas as chamadas de geração de texto. Esse endpoint roteia a requisição para a região com

> capacidade disponível, podendo incluir regiões fora do território nacional.
>
> Cabe esclarecer que, por determinação do Conselho Superior da Justiça do Trabalho (CSJT), toda a interação do sistema Galileu com serviços de inteligência artificial se dá através de serviço disponibilizado pelo CSJT, através do Contrato Estruturante de Nuvem estabelecido pelo Conselho e utilizado pela Justiça do Trabalho. (grifo do original)

Com base no exposto anteriormente, evidencia-se a possível ocorrência de transferência internacional de dados pessoais, inclusive de dados sensíveis, mediante o armazenamento desses dados no serviço de nuvem utilizado pelo Tribunal, conforme mencionado no item “a” deste achado.

Critérios de auditoria

- Lei nº 13.709/2018, artigos 5º, 33 e 35;
- Resolução CNJ nº 363/2021, artigo 1º;
- Instrução Normativa GSI/PR nº 5/2021, artigo 11 e 17;
- ABNT NBR ISO/IEC 27002:2022, itens 5.19 e 5.23;
- Resolução CD/ANPD nº 19/2024;
- Resolução CD/ANPD nº 32/2026;
- Acórdão TCU nº 1.372/2025 – Plenário (item 75 do Relatório).

Evidências

- Relatório de Feedback – Organização Tribunal Regional do Trabalho da 4ª Região, questão 8.1.2;
- RDI Seaudi nº 03/2026 (documento nº 14);
- Inventários de Dados Pessoais (IDP) compartilhados com a Seaudi. Levantamento (projeto piloto) realizado em unidades vinculadas à DG;
- Contrato TRT4 nº 16/2025 – PROAD nº 7676/2024;
- PROAD nº 704/2026;
- Política de Privacidade para o Google Workspace (tópico Estrutura de transferência de dados).

Possíveis causas

- Complexidade das normas e diretrizes relacionadas à proteção de dados pessoais, dificultando sua interpretação e aplicação prática pelas unidades envolvidas;

- Grau de maturidade em governança e gestão de riscos de privacidade e proteção de dados em processo de amadurecimento no Tribunal;
- Ausência de conhecimento consolidado dos procedimentos e das rotinas para tratamento e armazenamento de dados pessoais adotados pelas demais unidades administrativas do TRT4;
- Incerteza quanto à localização geográfica dos datacenters utilizados pela empresa provedora de serviços em nuvem.

Efeitos

- Risco à privacidade dos titulares dos dados tratados pelo Tribunal pelo vazamento de informações pessoais e dados sensíveis, decorrente de compartilhamento de dados pessoais com terceiros;
- Prejuízo à imagem e à confiança da instituição;
- Possibilidade de aplicação de sanções pela Agência Nacional de Proteção de Dados ou condenações judiciais para pagamento de indenizações;
- Possível descumprimento de normas de segurança da informação na utilização de serviços em nuvem;
- Eventual exposição dos dados pessoais tratados pelo Tribunal a ordenamentos jurídicos estrangeiros potencialmente incompatíveis com os requisitos e garantias previstos na LGPD.

Manifestação do Auditado

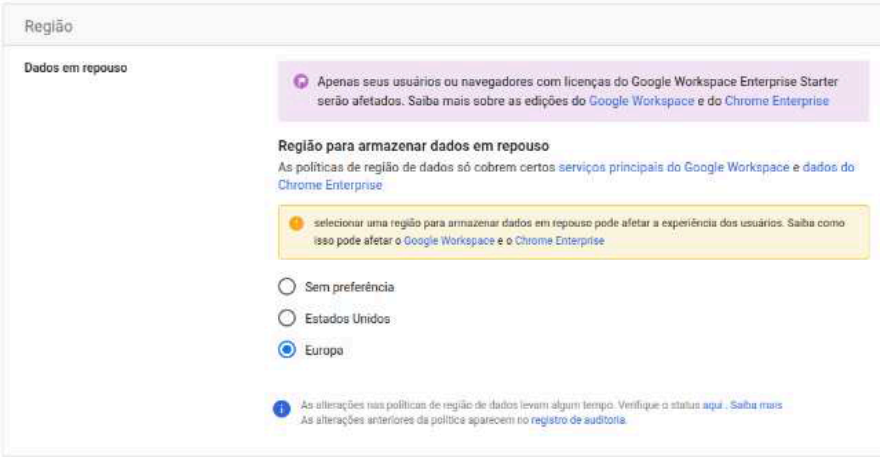
A DG, em sua manifestação, informou que (documento nº 27):

> Atualmente a Gestão de Riscos é focada nos ativos tecnológicos pensando nos riscos de segurança da informação: indisponibilidade, confidencialidade e integridade, **porém sem foco na LGPD**.
> Será criada uma **Gestão de Riscos em LGPD para o Google Workspace**, em paralelo a gestão de riscos de ativos executada atualmente, **focado exclusivamente em riscos relacionados à privacidade dos dados de titulares em serviços de nuvem que tratam desses dados**. Este foco deve-se a este ser o contrato principal onde identificou-se a presença de dados pessoais. **Essa gestão de riscos será incorporada oficialmente no ciclo do SGSI de 2028 a 2029**. (grifo nosso)

Quanto ao item “b” da situação encontrada, **foi apresentada uma nova evidência** em relação à hospedagem de dados no serviço de nuvem do Google Workspace. Sobre o item “b” a DG informou que (documento nº 27):

> Os contratos em geral já possuem cláusulas sobre LGPD, como vê-se no contrato 16/2025 com Google.

[...]
Com relação ao Google Workspace, especificamente, **já está configurado para que os dados em repouso fiquem hospedados na União Europeia, ficando assim em conformidade com a LGPD**, conforme página 57 do Relatório Preliminar enviado:



(grifo nosso)

Conclusão da Equipe de Auditoria

Inicialmente, destaca-se que a área técnica apresentou, em sua manifestação ao Relatório Preliminar, evidência de que o Google Workspace está configurado para armazenar os dados em repouso na União Europeia. Diante dessa nova informação – desconhecida à época da execução da auditoria – e considerando que a ANPD reconheceu que a União Europeia possui grau de proteção adequado para fins de transferência internacional de dados, em conformidade com o inciso I do artigo 33 da LGPD, **esta equipe de auditoria entende que não subsistem os fundamentos que justificavam a recomendação preliminar para esse item**.

Por outro lado, diante da situação relatada no item “a” do presente achado, esta equipe de auditoria considera pertinente manter recomendação correspondente a esse aspecto. A medida tem como objetivo aprimorar o tratamento de dados pessoais em serviços de armazenamento em nuvem, estruturando formalmente a análise de riscos e assegurando o alinhamento contínuo do TRT4 às normas de segurança da informação e à LGPD.

Proposta de Encaminhamento

R5. RECOMENDA-SE ao Tribunal Regional do Trabalho da 4ª Região que, a fim de mitigar o risco de possível descumprimento de normas de segurança da informação e de dano à privacidade dos titulares dos dados, realize o gerenciamento dos riscos

associados ao armazenamento de dados pessoais em serviços de nuvem, garantindo o alinhamento ao disposto na Instrução Normativa GSI/PR nº 5/2021 e na norma ABNT NBR ISO/IEC 27002:2022.

3. CONCLUSÃO

O presente trabalho teve como objetivo avaliar as medidas implementadas pelo TRT4 para adequação à Lei Geral de Proteção de Dados, em atendimento à recomendação do Tribunal de Contas da União para o envolvimento da Secretaria de Auditoria no processo de implementação dessa legislação no âmbito do Tribunal. Assim, o escopo do trabalho partiu do questionário elaborado pelo TCU – que foi organizado em duas questões de auditoria, englobando 11 subquestões e 36 itens avaliados.

Os resultados da auditoria evidenciaram que o TRT4 vem adotando medidas relevantes voltadas à implementação da LGPD, demonstrando comprometimento institucional com a proteção de dados pessoais. Destaca-se, em especial, a atuação do Encarregado pelo Tratamento de Dados Pessoais e da Assessoria de Otimização de Processos da Diretoria-Geral, responsável pelo suporte ao Subcomitê de Proteção de Dados Pessoais, na condução das iniciativas relacionadas ao tema.

Dos procedimentos realizados, a maior parte apresentou aderência aos critérios normativos adotados no trabalho. As oportunidades de melhoria identificadas deram origem às propostas de encaminhamento constantes deste relatório, voltadas ao fortalecimento da governança em proteção de dados pessoais, ao aprimoramento dos controles existentes e à mitigação dos riscos associados ao tratamento de dados pessoais no âmbito do TRT4. Registra-se, ainda, que algumas situações avaliadas não foram consideradas achados de auditoria, em razão do contexto normativo aplicável, das iniciativas já adotadas pela Administração e da necessidade de priorização das medidas com maior potencial de contribuição para o aprimoramento da proteção de dados pessoais no TRT4, conforme detalhado no Apêndice A deste relatório.

Após a análise das manifestações da unidade auditada ao Relatório Preliminar de Auditoria, foram consolidadas cinco propostas de encaminhamento

destinadas ao aperfeiçoamento dos processos adotados pelo TRT4 para atendimento da LGPD. Destaca-se que a unidade auditada, de modo geral, considerou oportunas as recomendações apresentadas e informou a existência de iniciativas já em andamento para mitigação dos riscos identificados.

Por fim, a realização deste trabalho reafirma o papel da Secretaria de Auditoria no apoio ao aprimoramento da governança institucional, da gestão de riscos e da conformidade normativa, contribuindo para o fortalecimento da proteção de dados pessoais e para o alcance dos objetivos estratégicos do Tribunal.

4. ENCAMINHAMENTO

Em consonância com o papel da auditoria interna estabelecido na Resolução CNJ nº 309/2020, na Resolução CSJT nº 282/2021 e na Resolução Administrativa TRT4 nº 03/2021, submetemos à consideração de Vossa Excelência o resultado desta auditoria, sugerindo que seja determinada à área auditada a elaboração de **plano de ação** para implementação das propostas de encaminhamento acolhidas, nos termos do §1º do artigo 21 da Portaria GP.TRT4 nº 3.215/2024.

Em 24 de julho de 2026.

Documento assinado digitalmente
Adriano Prado Cavalheiro
Equipe de Auditoria
Divisão de Auditoria de Contratações

Documento assinado digitalmente
Pérola Priscila da Silva Rocha
Equipe de Auditoria
Divisão de Auditoria de Contratações

Documento assinado digitalmente
José Cláudio da Rosa Riccardi
Auditor responsável
Divisão de Auditoria de Contratações

Documento assinado digitalmente
Carolina Feuerharmel Litvin
Supervisora
Diretora da Secretaria de Auditoria

APÊNDICE A – RESPOSTAS ÀS QUESTÕES DE AUDITORIA

QUESTÕES DE AUDITORIA

1ª Questão de Auditoria: As iniciativas adotadas para adequação à LGDP, no âmbito do TRT4, atendem ao disposto na legislação?

Subquestão de Auditoria	Procedimento	Resposta da Seaudi
1.1. Foram elaboradas políticas relacionadas ao tratamento de dados pessoais?	a) Verificar se há Política de Classificação da Informação: i) Verificar se a política de classificação da informação abrange a categorização de dados pessoais. ii) Verificar se a política de classificação da informação contempla diretrizes quanto à identificação de dados pessoais sensíveis. iii) Verificar se a política de classificação da informação contempla diretrizes quanto à identificação de dados de crianças e adolescentes.	**Não.** O Tribunal de Contas da União (TCU) destaca a importância da formalização de políticas voltadas à segurança da informação e à proteção de dados pessoais. Nesse contexto, a Política de Classificação da Informação estabelece diretrizes para assegurar que as diferentes informações recebam níveis adequados de proteção, de acordo com sua importância e os riscos associados. No que tange à classificação da informação, o TCU ressalta que a LGPD demanda a adoção de controles específicos para o tratamento de dados pessoais sensíveis e de dados pessoais de crianças e adolescentes. Embora o TRT4 não possua um normativo específico de Política de Classificação da Informação sob a perspectiva da LGPD, a equipe de auditoria deliberou por não considerar a situação como achado e nem propor oportunidade de melhoria para esse questionamento. Conforme resposta da área técnica à RDI Seaudi nº 03/2026 (documento nº 14), a Resolução Administrativa nº 01/2017, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI) no âmbito do TRT4 "[...] contempla, de forma geral, a proteção de dados pessoais, **sem estabelecer regramento específico para o tratamento de dados pessoais sensíveis, bem como de dados de crianças e adolescentes**." (grifo nosso). Destaca-se, ainda, que nem o Conselho Nacional de Justiça, nem o Conselho Superior da Justiça do Trabalho exigem, em suas respectivas normas, a formalização de política específica de classificação da informação. A Resolução CNJ nº 363/2021 determina a elaboração de uma Política Geral de Privacidade e Proteção de Dados Pessoais (artigo 1º, inciso, VI, alínea "c")

		e de uma Política de Segurança da Informação (artigo 1º, inciso XI, alínea “a”). Já a Resolução CSJT nº 309/2021, determina apenas a elaboração de Políticas de Privacidade e Proteção de Dados Pessoais no âmbito dos TRTs (artigo 1º).
	b) Para a Política de Privacidade e Proteção de Dados Pessoais, instituída pela Portaria GP.TRT4 nº 2.036/2021, verificar se ela: i) prevê a relação com outros normativos associados (ex.: Política de Segurança da Informação); ii) regulamenta os agentes de tratamento no âmbito do TRT4; iii) define gestores(as) e estruturas, atribuindo-lhes papéis e responsabilidades pela proteção de dados pessoais; iv) abrange e é aplicável aos(às) fornecedores(as) do TRT4 que tratem dados pessoais; v) regulamenta os principais aspectos para a proteção de dados pessoais na organização (tratando, no mínimo, das hipóteses de tratamento de dados pessoais utilizadas, do exercício dos direitos dos titulares, das transferências e compartilhamentos de dados e da interação com a ANPD; vi) prevê a necessidade de comunicação/conscientização aos(às) interessados(as); vii) prevê a sua revisão periódica ou quando ocorrerem mudanças significativas.	**Sim**
	c) Verificar se as políticas relacionadas ao tratamento de dados pessoais são revistas em intervalos planejados (Política de Segurança da Informação, Política de Classificação da Informação, Política de Privacidade e Proteção de Dados Pessoais, Programa de Governança em Privacidade de	**Não.** Inicialmente, destaca-se que a Política de Segurança da Informação (PSI) vem sendo revisada periodicamente, conforme verificado pelas diversas portarias alteradoras publicadas ao longo dos últimos anos. Quanto à **Política de Privacidade e Proteção de Dados Pessoais** e ao **Programa de Governança em Privacidade de Dados**, não foram

	Dados).	identificadas evidências de revisões periódicas desses documentos. A Política de Privacidade e Proteção de Dados Pessoais, instituída pela Portaria GP.TRT4 nº 2.036/2021, prevê, em seu artigo 22, que a revisão deve ser realizada em intervalos planejados e não superiores a 12 meses. Já no Programa Institucional de Governança em Privacidade de Dados, instituído pela Portaria GP.TRT4 nº 4.948/2022, o Tribunal assumiu o compromisso de revisão periódica do documento. Entretanto, em resposta à RDI Seaudi nº 03/2026 (documento nº 14), a área técnica informou que, diante dessas constatações, já está adotando medidas para sanar essas pendências e que as atualizações previstas para os normativos possuem caráter predominantemente formal. Destacou, ainda, que aguarda a publicação da atualização da Resolução CSJT nº 309/2021, que estabelece diretrizes e orientações para a formulação de Políticas de Privacidade e Proteção de Dados Pessoais no âmbito dos Tribunais Regionais do Trabalho. Também informou que os membros do Subcomitê de Proteção de Dados Pessoais, referentes ao biênio 2026-2027 irão elaborar um Plano de Ação para 2026, que irá contemplar, dentre outros tópicos, a revisão dessas políticas. Diante dessas informações e considerando as medidas já iniciadas pela Administração, a equipe de auditoria decidiu por não considerar a situação relatada anteriormente como um achado e nem apresentar uma oportunidade de melhoria.
1.2. Foram conduzidas iniciativas para providenciar a adequação do Tribunal à LGPD?	a) Verificar se foi instituído projeto, plano de ação ou iniciativa similar para providenciar a adequação à LGPD;	**Sim**
	b) Verificar se foram publicados normativos que tratam dos aspectos mais importantes relacionados à proteção de dados e à privacidade;	**Sim**
	c) Verificar se o Tribunal mapeou seus processos de tratamento de dados e instituiu programa de governança em privacidade de dados.	**Sim, exceto para o mapeamento de processo de tratamento de dados – Achado A2**. O Tribunal instituiu seu Programa Institucional de Governança em Privacidade de

		Dados (Portaria GP.TRT4 nº 4.948/2022). Contudo, até o momento, o mapeamento do tratamento de dados foi realizado apenas em oito unidades à época vinculadas à Diretoria-Geral, dentro do escopo de um projeto piloto. Em resposta à RDI Seaudi nº 03/2026 (documento nº 14), a área técnica esclareceu que essa etapa inicial permitiu testar e validar a adequação do modelo de inventário proposto e avaliar a efetividade das informações coletadas. Informou, ainda, que foram realizados contatos com o Tribunal Regional do Trabalho da 21ª Região para conhecimento das práticas adotadas em relação ao formulário de mapeamento. Adicionalmente, a área destacou que pretende fazer uma segunda rodada de mapeamento de processos, ainda restrita às unidades subordinadas à DG, com o objetivo de aperfeiçoar o *template* do Inventário de Dados Pessoais (IDP) utilizado. Após a aprovação desse novo modelo, planeja-se a expansão do mapeamento, com a aplicação do IDP em outras áreas do Tribunal, bem como a elaboração do Relatório de Impacto à Proteção de Dados (RIPD).
1.3. Foram identificados outros normativos que abrangem comandos que remetem à proteção de dados pessoais e que também devem ser seguidos pelo Tribunal?	a) Verificar se a instituição identificou, além da LGPD, outras leis, regulamentos e instruções normativas que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados.	**Sim**
1.4. Há iniciativas para conscientização e capacitação dos(as) magistrados(as) e dos(as) servidores(as) em proteção de dados pessoais no âmbito do TRT4?	a) Solicitar os planos de conscientização e/ou de capacitação dos(as) servidores(as) e dos(as) magistrados(as) dos últimos três anos: i) Avaliar se os planos contemplaram a temática de proteção de dados pessoais; ii) Solicitar a lista de participantes dos treinamentos. b) Verificar se foram considerados diferentes níveis de capacitação, de acordo com o envolvimento do servidor(a) na temática de proteção de dados pessoais;	**Não. Achado A1.**

	c) Levantar quais as áreas e os(as) respectivos(as) magistrados(as) e servidores(as) que atuam diretamente em atividades que realizam tratamento de dados pessoais; d) Verificar se os(as) magistrados(as) e os(as) servidores(as) envolvidos(as) diretamente em atividades que realizam tratamento de dados pessoais receberam treinamento relacionado à proteção de dados pessoais.	
1.5. Foram identificadas as principais partes interessadas relacionadas à proteção de dados pessoais do Tribunal?	a) Verificar se foram identificados os **operadores** de dados pessoais; b) Verificar se foram identificadas as categorias de **titulares** de dados pessoais; c) Verificar se foi(foram) identificado(s), quando for o caso, **controlador(es) conjunto(s)**.	**Sim.** Destaca-se que, para o caso de controladores conjuntos, a verificação realizada restringiu-se às contratações administrativas típicas deste Tribunal, conforme manifestação da área técnica para a RDI Seaudi nº 03/2026 (documento nº 14). Para essas situações, não foram identificados controladores conjuntos. Adicionalmente, da análise de acordos de cooperação técnica assinados pelo TRT4 com outros órgãos e instituições, em 2025, verificou-se que os partícipes figuram como controladores dos seus próprios dados e operadores em relação aos dados fornecidos para seu tratamento.
1.6. Foram identificados os dados pessoais que são tratados pelo TRT4, bem como os processos que realizam esses tratamentos?	a) Verificar se foram identificados os **processos de negócio** que realizam tratamento de dados pessoais; b) Verificar se foram identificados os **responsáveis** pelos processos que realizam tratamento de dados pessoais; c) Verificar se foram identificados os **dados pessoais** que são tratados pela organização; d) Verificar se foram identificados os **locais** onde os dados pessoais são armazenados (ativos ou nuvem); e) Verificar se foram identificados os **riscos** associados ao processo de tratamento de dados.	**Não. Achado A2**

2ª Questão de Auditoria: A implementação de medidas e controles de proteção de dados pessoais, no âmbito do TRT4, atendem ao disposto na LGPD e demais normas aplicáveis?

Subquestão de Auditoria	Procedimento	Resposta da Seaudi
2.1. O tratamento de dados pessoais é realizado em conformidade com a LGPD?	a) Levantar quais processos realizam tratamento de dados pessoais; b) Verificar se os processos que realizam tratamento de dados pessoais estão em conformidade com os princípios da finalidade e da necessidade (minimização e tempo de retenção) estabelecidos na LGPD; c) Verificar se os processos que realizam tratamento de dados pessoais o fazem dentro das hipóteses legais, bem como se há registro das operações de tratamento de dados pessoais que são realizadas; d) Verificar se existe(m) inventário(s) de dados pessoais que consolida(m) os registros de atividades de tratamento de dados pessoais;	**Não para os itens "b" e "d". Achado A2.**
	e) Verificar se foi elaborado algum Relatório(s) de Impacto à Proteção de Dados Pessoais (RIPD);	**Não. Achado A3.**
	f) Existindo RIPDs, verificar se já foram implementados controles para mitigar os riscos identificados.	**Não se aplica.**
2.2. Foi realizada a identificação dos casos de transferência, compartilhamento ou tratamento conjunto de dados pessoais?	a) Verificar se o Tribunal identificou os casos de compartilhamento de dados com terceiros. Nesses casos, avaliar: i) se os papéis e responsabilidades estão definidos; ii) se houve adequação de contratos ou ajustes firmados com os operadores; iii) avaliar a adequação dos operadores à LGPD;	**Sim.**
	b) Avaliar se o Tribunal realiza transferência internacional de dados e se há atendimento ao disposto na LGPD; c) Verificar se o Tribunal realiza tratamento de dados pessoais em solução de computação em nuvem. Em	**Não. Achado A4.**

	caso positivo, avaliar: i) se há armazenamento de dados em território estrangeiro. Em caso positivo, avaliar se as práticas estão alinhadas à legislação brasileira; ii) se foi realizada avaliação dos riscos relativos a esse tratamento e se o gerenciamento de riscos atende aos critérios da norma; iii) a adequação dos instrumentos contratuais com os provedores de nuvem.	
	d) Nos casos em que há controladores conjuntos, verificar se os papéis e responsabilidades de cada um foram estabelecidos de forma transparente;	**Não se aplica**. Conforme descrito na subquestão 1.5, não foram identificados controladores conjuntos atuando com o Tribunal nas decisões referentes ao tratamento de dados pessoais.
2.3. São disponibilizados mecanismos para informar e dar atendimento aos direitos dos titulares de dados?	a) Para a Política de Privacidade e Proteção de Dados Pessoais, instituída pela Portaria GP.TRT4 nº 2.036/2021, verificar se ela: i) está publicada em local de fácil acesso; ii) informa o titular de dados sobre os princípios aplicáveis ao tratamento de dados pessoais; iii) contém informações sobre o controlador, o operador e o encarregado; iv) informa como se dá a custódia de dados pessoais; v) informa sobre como o titular de dados pode obter as informações previstas no artigo 18 da LGPD, quando aplicáveis; vi) informa sobre como o titular de dados pode exercer seus direitos; vii) informa quais são as hipóteses em que, no exercício de suas competências, a organização realiza o tratamento de dados pessoais; viii) fornece informações claras sobre a previsão legal, a finalidade, as informações de contato do controlador, os procedimentos e as	**Sim.**

	práticas utilizadas no tratamento de dados; ix) fornece informações acerca do uso compartilhado de dados pelo controlador e sua finalidade; x) informa a data de sua última atualização; b) Verificar se foi definido um fluxo, alinhado ao disposto na norma do CSJT, para atendimento aos direitos dos titulares, desde o ingresso da solicitação até o fornecimento da respectiva resposta; c) Avaliar se foi criado um site com informações sobre a LGPD, contendo as informações exigidas em norma. d) Verificar se foram implementados mecanismos para atender os direitos do titular, relacionados à obtenção de informações sobre o tratamento dos dados, bem como sobre os seus dados específicos e o respectivo tratamento; e) Verificar se foram estipulados prazos para atendimento de cada um dos direitos dos titulares.	
2.4. Foram instituídos mecanismos para o tratamento de violações de dados pessoais?	a) Verificar se foram instituídos processos para resposta a incidentes de segurança da informação que envolvam violação de dados pessoais; b) Verificar se foram instituídos meios para registro, inclusive pelos próprios titulares, de incidentes de segurança da informação que envolvam violação de dados pessoais; c) Verificar se há monitoramento contínuo da ocorrência de eventos que podem estar associados a incidentes de segurança da informação que envolvam violação de dados pessoais; d) Verificar se foi estabelecido procedimento, com prazos e responsabilidades definidos, para a comunicação de incidentes à ANPD e aos titulares dos dados.	**Sim.**
2.5. Foram instituídas medidas para tratamento de riscos	a) Verificar se foram adotadas medidas de segurança, técnicas (soluções de segurança, controle de	**Sim**. Quanto à existência de processo formal de registro, cancelamento e provisionamento de acesso de usuários a

relacionados à proteção de dados pessoais?	acesso) e administrativas (medidas organizacionais), para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, em especial para: i) Verificar se foram definidos papéis, responsabilidade e procedimentos específicos para esse propósito; ii) Verificar se existe um processo formal de registro, cancelamento e provisionamento de acesso de usuários a sistemas que realizam tratamento de dados pessoais; iii) Verificar se há rastreabilidade (logs) dos tratamentos de dados efetuados; iv) Verificar se é utilizada criptografia para proteger os dados pessoais, em especial os dados pessoais sensíveis.	sistemas que realizam tratamento de dados pessoais, verificou-se que esse processo está descrito no item 6 (Do controle do acesso) do Anexo III (Uso de Recursos de Tecnologia da Informação e Controle de Acesso) da PSI, instituída pela Portaria GP.TRT4 nº 2.697/2025. Para cumprimento do disposto na PSI, a Secretaria-Geral de Tecnologia da Informação, anualmente, encaminha um e-mail aos(às) gestores(as) das unidades para revisão de acessos aos recursos de TI relacionados a alguns sistemas que armazenam dados pessoais, como ADMEletrônico e PROAD. Entretanto, para a maioria dos sistemas que realizam tratamento de dados pessoais, verificou-se que a concessão, alteração e revogação de acessos são realizadas por servidores(as) designados(as) como gestores(as) dos respectivos produtos, nos termos da Portaria GP.TRT4 nº 2.338/2021. Em resposta à RDI Seaudi nº 06/2026 (documento nº 18), a Divisão de Governança de Dados (DGD) esclareceu os procedimentos adotados para os sistemas SIGEP-JT e Portal de Apoio ao SIGEP-JT (PAS). Conforme informado, a concessão de acesso ocorre por meio de requisição formal do gestor da unidade interessada, com indicação do(a) usuário(a) e da justificativa funcional. Já a revogação dos acessos ocorre por “solicitação do gestor da unidade, quando cessada a necessidade do perfil, ou em razão de remoção da unidade, de desligamento (aposentadoria, exoneração ou término de requisição/cessão, óbito), promovendo a DGD a revogação dos perfis, bem como, quando das revisões periódicas”. Nesse aspecto, destaca-se que a PSI atribui à chefia imediata a responsabilidade de solicitar a remoção dos acessos concedidos a servidores(as) e estagiários(as) imediatamente após o afastamento ou desligamento da unidade. A DGD informou, contudo, que reconhece que “essa comunicação nem sempre ocorre de forma tempestiva, razão pela qual são adotados controles detectivos para mitigar o risco de manutenção de acessos indevidos, como a revisão semanal das movimentações”. Dessa forma, observou-se que os procedimentos de concessão e revogação de acessos podem apresentar

		particularidades conforme o sistema administrativo considerado. Entretanto, considerando os controles adotados pela DGD, bem como o fato de que os Inventários de Dados Pessoais contemplam a avaliação do risco 15.1 – Acesso não autorizado, esta equipe de auditoria decidiu por não caracterizar a situação relatada como um achado de auditoria. Quanto à utilização de criptografia para proteger os dados pessoais, em especial os dados pessoais sensíveis, são utilizados para dados em trânsito na rede interna ou na internet. Conforme informado pela área técnica, em resposta à RDI Seaudi nº 03/2026 (documento nº 14) “Os sistemas utilizam protocolo HTTPS [*Hyper Text Transfer Protocol Secure*, ou Protocolo de Transferência Segura de Hiper Textos, em tradução livre] o que garante a confidencialidade, a integridade e autenticidade da conexão, protegendo todos os dados em trânsito.”.
	b) Verificar se foram adotadas as providências para que processos e sistemas sejam projetados (desde a concepção) de forma que a coleta e o tratamento de dados pessoais estejam limitados ao que é estritamente necessário para o propósito identificado (Privacy by design e Privacy by default).	**Sim.**