

ATA DE REUNIÃO – 17-3-2021

COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS – CGPDP

ASSUNTO/PROJETO	5ª REUNIÃO DO CGPD
DATA	17-03-2021, a partir das 14h30min
LOCAL	Google Meeting

PRESENTES À REUNIÃO

NOME	CARGO / ÁREA
Roberto Masami Nakajo	Magistrado Gestor Estratégico de Metas Coordenador
Dilcionir José Furlan	DIGER
Alcino Ecker Junior	SECOR
Valdir Luiz da Cunha	SETIC
Gilmar Edilson Vieira	ASJUR
Hamilton José Maestri	SEGEPE
Daniele Priscila Rodrigues de Oliveira	SECOM
Alex Cristiano Gramkow Hammes	SEAUD
Denise Maria Lucena Zacchi	Vice-Presidência/OUVIDORIA
Anderson Bastos	SETIC/SEINFRA
Arthur Fernando Dellagiustina Lago	SETIC/SEINFRA
Karoline da Cunha Vieira	DIGER

AUSÊNCIAS JUSTIFICADAS

Alcino Ecker Junior	SECOR
---------------------	-------

ASSUNTOS TRATADOS

A reunião iniciou-se às 14h40min

A servidora Karoline iniciou a reunião apresentando as ações relativas à LGPD realizadas desde a última reunião do CGPD e apresentou os objetivos da reunião:



ATA DE REUNIÃO – 17-3-2021

COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS – CGPDP

1 - Analisar o formulário do Tribunal de Contas da União que trata de Auditoria com objetivo de avaliar a adequação das organizações públicas federais à Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) (PROAD 2099/2021) e as respostas pertinentes;

2 - Analisar o Plano de Ação para implementação da LGPD reformulado - adequado à Resolução CNJ n. 363/2021 e exigências do TCU;

A palavra foi passada ao Diretor da Secretaria de Auditoria (SEAUD), Alex Cristiano Gramkow Hammes, que apresentou breve explicação acerca da forma como o TCU conduz os trabalhos nas auditorias semelhantes à noticiada acima.

Foi esclarecido que, nesse momento, o preenchimento do formulário servirá para coleta de informações e que posteriormente a Corte de Contas poderá, ou não, determinar a observância dos itens constantes do documento.

Após sua explicação, o Diretor ausentou-se da reunião.

Os demais participantes passaram a analisar os itens do formulário do TCU (anexo a presente ata).

Dos itens analisados, destacam-se as ações a serem realizadas quanto aos seguintes itens:

item 3.3 - A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?

O CGPD concordou com a identificação dos operados nos moldes realizados no Ato Conjunto TST.CSJT.GP Nº 4, DE 12 DE MARÇO DE 2021 (art. 14 e art. 18).

Caberá à **SETIC** apresentar minuta de documento para validação e publicação até 30-3-2021 (prazo para envio do formulário ao TCU).

item 3.4 - A organização avaliou se há tratamento de dados que envolva controlador conjunto?

Será realizada consulta o TCU para esclarecimento quanto a questão. Em princípio, entendeu-se que, em razão da autonomia administrativa dos Tribunais este item não se aplicaria ao Tribunal.

Caberá a **DIGER** realizar a consulta.

item 5.1 - A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?



ATA DE REUNIÃO – 17-3-2021

COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS – CGPDP

A Diretora da SECOM apresentou proposta para elaboração de um plano de conscientização em parceria com o SEDUC e a Escola Judicial, com medidas iniciais para o 1º semestre.

A partir do 2º semestre, a medida que forem sendo tomadas decisões e for possível aprofundar a capacitação, serão estudadas novas ações.

A ação será incorporada ao Plano de Ação da LGPD (PROAD 8737/2019) e deverá ser apresentada em tempo hábil para sua aprovação até 30-3-2021.

Ficarão responsáveis pela ação: **SECOM, SGP/SEDUC e Escola Judicial.**

Item 10.2 - A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?

Item 10.5 - A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (Privacy by Design e Privacy by Default)?

A área técnica (**SETIC**) avaliará essas duas questões, de modo que seja possível identificar a resposta mais correta aos itens.

Finalizada a análise do formulário do TCU, passou-se à análise do Plano de Ação de implementação à LGPD reformulado - com adequações à Resolução CNJ n. 363/2021 e exigências do TCU.

A servidora Karoline esclareceu que quando do atendimento da Recomendação CNJ n. 73/2020 foram elaborados 6 Planos de Ações, um para cada tema abordado no inciso I do art. 1º da Norma (organização e comunicação; direitos do titular; gestão de consentimento; retenção de dados e cópia de segurança; contratos e plano de respostas a incidentes de segurança com dados pessoais).

Pontuou que muitas ações se repetiam em mais de um Plano e, com intuito de facilitar o entendimento do Plano, diante das Previsões da Resolução CNJ n. 363/2021, especialmente do inciso III do art. 2º, que recomenda a elaboração de plano de ação (Roadmap), com a previsão de todas as atividades constantes nesta Resolução, o Plano foi reformulado num único documento em forma de tabela, com indicação das ações, fundamentação legal/normativa, prazo para realização e área responsável.

O plano traz as ações anteriormente já planejadas, com adequações necessárias ao atendimento da Resolução n. 363/2021.

A servidora trouxe os seguintes itens para discussão ao grupo:



ATA DE REUNIÃO – 17-3-2021

COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS – CGPDP

- **inciso XII do art. 1º da Resolução (elaborar e manter os registros de tratamentos de dados pessoais)** - somente depois de se mapear os dados e realizar o inventário será possível adentrar nesse item, porque saberemos o universo de dados a serem registrados.

Porém, remanesce dúvida sobre os papéis dos Conselhos e do TRT 12 nessa ação.

O Diretor-Geral informou que na próxima reunião de Diretores-Gerais dos Tribunais do Trabalho será levada questão relacionada à LGPD.

Assim, deliberou-se por aguardar e reavaliar em momento posterior eventual provocação dos Conselhos sobre o tema.

- **ação 17 - Identificar e revisar as normas internas impactadas pela LGPD** - foi realizada discussão sobre como a ação poderia ser conduzida.

Após breve debate, sugeriu-se a elaboração de um check-list para envio a todas as áreas que utilizam, na gestão de suas atividades, Portarias internas, para realização de levantamento daquelas que precisariam ser revisadas e adequadas à LGPD.

O Assessor Jurídico ponderou que a medida já inicia o mapeamento de dados, na medida em que identificará as áreas que atuam com dados pessoais.

Ficou registrado que a DIGER ficará responsável pela operacionalização da ação, com auxílio da Assessoria Jurídica para elaboração do Check-list.

A DIGER realizará ajuste no Plano de Ação para constar do documento a realização das atividades acima.

- **Tratamento dos dados pessoais dos magistrados e servidores:** discutiu-se a pertinência de iniciar medidas necessárias ao tratamento de dados pessoais pelas áreas do Tribunal, especialmente nas situações em que seria necessário colher o consentimento, na forma do inciso I do art. 7º da LGPD.

A Diretora da SECOM apresentou exemplos de situações em que seria necessário o consentimento de servidores para divulgação de dados pessoais em matérias da SECOM e ações da Memória do Tribunal.

O grupo concordou que para adequação à LGPD, seria necessária adoção de um modelo de consentimento para utilização pelas áreas nessas situações.

Ficou registrado que a DIGER ficará responsável pela ação, com auxílio da Assessoria Jurídica e Secretaria de Gestão de Pessoas para elaboração do Termo.



ATA DE REUNIÃO – 17-3-2021

COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS – CGPDP

A DIGER realizará ajuste no Plano de Ação para constar ação preventivo tal medida.

Por fim, foi deliberado que, após ajustes necessários (nos termos acima indicados) o Plano de Ação será submetido para aprovação do CGPD e, posteriormente, à Presidência, em tempo hábil, de modo que esteja ratificado até 30-3-2021, para sua remessa ao TCU.

A reunião foi encerrada às 16h:30min

FECHAMENTO DA ATA

DATA	NOME DO REDATOR	CONTATO
18-3-2021	Karoline da Cunha Vieira	3216-4194



Questão/Item de Auditoria do TCU	Observação sobre o item (TCU)	Respostas Disponíveis	Resposta do TRT12	Observação
1. Identificação do respondente				
1.1 Dados do servidor responsável pela resposta ao questionário:	Os dados pessoais solicitados se limitam ao que é estritamente necessário para que a equipe de auditoria possa entrar em contato com o respondente caso haja necessidade.		Servidora Responsável: Karoline da Cunha Vieira - DIGER	Marcador 2 do PROAD 2099/2021
2. Preparação				
Antes de iniciar o processo de adequação à LGPD, a organização deve adotar medidas para construir um ambiente propício para o sucesso da iniciativa.				
2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?	Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 5.4. A organização deve conduzir iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD. Um exemplo de iniciativa pode ser a instituição de comitê ou grupo de trabalho. É importante que a iniciativa conte com o apoio ou, até mesmo, com a participação direta da alta direção da organização. Ademais, convém que sejam envolvidas pessoas pertencentes a unidades que exercem atividades relevantes para o tratamento de dados pessoais (e.g.: Segurança da Informação, Tecnologia da Informação, Direito, Auditoria/Conformidade e Ouvidoria). Um exemplo de artefato que pode ser produzido pela iniciativa é o plano de ação.	Sim (a organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD). Parcialmente (a organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD). Não.	Sim (a organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD).	
2.2 A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?	Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 5.4. A organização deve documentar informações relacionadas aos objetivos da iniciativa de adequação e às ações necessárias para alcançá-los.	Sim Não	Sim	
2.2.1 Anexe o plano de ação, plano de projeto ou documento similar que foi elaborado pela organização:	Só responder essa pergunta sob as seguintes condições: A resposta foi 'Sim' na questão '3 [Q22]' (2.2 A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?)	Carregar arquivo comprovando a elaboração do Plano de Ação (Só é aceito o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)		Aguardar o final do prazo e juntar o Plano de Ação revisado - PROAD 8737/2019
3. Contexto organizacional				
Para alcançar os resultados pretendidos pela iniciativa de adequação à LGPD, a organização deve avaliar questões internas e externas que são relevantes para atingir os objetivos.				
3.1 A organização conduziu iniciativa para identificar outros normativos (e.g.: leis, regulamentos e instruções normativas), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?	Referência(s): ABNT NBR ISO/IEC 27.701/2019, item 5.2.1. Além da LGPD, há outros normativos que abordam o tratamento de dados pessoais e que também devem ser respeitados por determinadas organizações. O Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Consolidação das Leis Trabalhistas (CLT), a Lei de Acesso à Informação e a Lei 13.787/2018 (que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente) são alguns exemplos desses normativos.	Sim Não	Sim	Seguimos a legislação e normativos dos Conselhos Superiores que abordam tratamento de dados. Devem ser mencionadas as resoluções CNJ 360, 361, 362 e 363.
3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?	Referência(s): Lei 13.709/2018, art. 5º, inciso V. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.2 e 7.2.8. Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos. O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Os titulares podem ser enquadrados em diferentes categorias como: cidadão, cliente, servidor público, representante de fornecedor e terceirizado.	Sim (todas as categorias de titulares de dados pessoais foram identificadas). Parcialmente (algumas categorias de titulares de dados pessoais foram identificadas). Não (ainda não foi conduzida iniciativa para identificar as categorias de titulares de dados pessoais).	Não (ainda não foi conduzida iniciativa para identificar as categorias de titulares de dados pessoais).	O plano de ação juntado ao PROAD 8737/2019 contempla, como um dos itens, o mapeamento de dados. A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização. Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.
3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?	Referência(s): Lei 13.703/2018, art. 5º, incisos VI e VII. ABNT NBR ISO/IEC 27.701/2019, item 5.2.2. Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos. O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, este, por sua vez, é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.	Sim (a iniciativa foi concluída e todos os operadores foram identificados). Sim (a iniciativa foi concluída e a organização constatou que não há operadores que realizam tratamentos de dados pessoais em seu nome). Parcialmente (a iniciativa ainda está em andamento). Não (ainda não foi conduzida iniciativa para identificar os operadores).		Deverá ser editada Norma, nos termos do Ato CONJUNTO TST.CSJT.GP Nº 4, DE 12 DE MARÇO DE 2021 (art. 14 e art. 18) - identificando os operadores. Com a publicação do normativo, o item estará atendido. Responsabilidade: SETIC.
3.3.1 A organização adequou os contratos firmados com os operadores identificados de forma a estabelecer suas responsabilidades e papéis com relação à proteção de dados pessoais?	Só responder essa pergunta sob as seguintes condições: A resposta foi 'Sim (a iniciativa foi concluída e todos os operadores foram identificados),' na questão '7 [Q33]' (3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?) Referência(s): Lei 13.709/2018, art. 39; arts. 42-46. ABNT NBR ISO/IEC 27.701/2019, item 7.2.6. O controlador deve ter contrato firmado com os operadores de dados pessoais para assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais que são compartilhados com eles.	Sim (A organização adequou todos os contratos firmados com os operadores que foram identificados). Parcialmente (A organização adequou os contratos firmados com alguns operadores que foram identificados). Não (A organização não adequou os contratos firmados com os operadores que foram identificados).	Não (A organização não adequou os contratos firmados com os operadores que foram identificados).	No plano de ação aprovado no PROAD 8737/2019 (PP 936/2021) relativo à adequação dos contratos à LGPD, está sendo feito mapeamento dos contratos e as medidas necessárias para adequação à LGPD.



3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?	<p>Referência(s): Lei 13.709/2018, art. 5º, inciso VI; art. 7º, § 5º. ABNT NBR ISO/IEC 27.701/2019, itens 5.2.2 e 7.2.7.</p> <p>Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos.</p> <p>O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Por sua vez, controlador conjunto é o controlador de dados pessoais que determina os propósitos e as formas do tratamento de dados pessoais junto com outro(s) controlador(es).</p>	<p>Sim</p> <p>Não</p>	<p>Não</p>	<p>Em razão da autonomia administrativa dos Tribunais - não seria um item que nos aplicaria - por isso a resposta não.</p> <p>Sem prejuízo, solicitar esclarecimento ao TCU sobre o que seria esse conceito de controlado compartilhado.</p>
3.4.1 Caso exista controlador conjunto, os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '9 [Q34]' (3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?)</p> <p>Referência(s): Lei 13.709/2018, arts. 42-45. ABNT NBR ISO/IEC 27.701/2019, item 7.2.7.</p> <p>É conveniente que a organização estabeleça formalmente os papéis e as responsabilidades de cada controlador caso haja controlador conjunto.</p> <p>Caso não haja tratamento de dados que envolva controlador conjunto, assinale a alternativa "não se aplica".</p>	<p>Sim (os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar).</p> <p>Parcialmente (há acordo de cooperação ou instrumento similar firmado, mas nem todos os papéis e responsabilidades de cada um dos controladores estão definidos).</p> <p>Não (os papéis e responsabilidades de cada um dos controladores não estão definidos em contrato, acordo de cooperação ou instrumento similar).</p> <p>Não se aplica (não há relação da organização com controlador conjunto).</p>	<p>Condicional a resposta anterior</p>	
3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?	<p>Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.</p> <p>O tratamento de dados pessoais envolve 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.</p>	<p>Sim (todos os processos de negócio que realizam tratamento de dados pessoais foram identificados).</p> <p>Parcialmente (alguns processos de negócio que realizam tratamento de dados pessoais foram identificados).</p> <p>Não (ainda não foi conduzida iniciativa para identificar os processos de negócio que realizam tratamento de dados pessoais).</p>	<p>Não (ainda não foi conduzida iniciativa para identificar os processos de negócio que realizam tratamento de dados pessoais).</p>	<p>O plano de ação juntado ao PROAD 8737/2019 contempla, como um dos itens, o mapeamento de dados.</p> <p>A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização.</p> <p>Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.</p>
3.5.1 A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim (todos os processos de negócio que realizam tratamento de dados pessoais foram identificados),' ou 'Parcialmente (alguns processos de negócio que realizam tratamento de dados pessoais foram identificados),' na questão '11 [Q35]' (3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?)</p>	<p>Sim (a organização identificou os responsáveis por todos os processos de negócio que realizam tratamento de dados pessoais e que já foram identificados).</p> <p>Parcialmente (a organização identificou os responsáveis por alguns dos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados).</p> <p>Não (a organização não identificou os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados).</p>	<p>Condicional a resposta anterior</p>	
3.6 A organização identificou quais são os dados pessoais tratados por ela?	<p>Referência(s): Lei 13.709/2018, art. 5º, inciso I; art. 37. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.2 e 7.2.8.</p> <p>O dado pessoal é uma informação relacionada à pessoa natural identificada ou identificável, como nome, RG e CPF.</p>	<p>Sim (todos os dados pessoais tratados pela organização foram identificados).</p> <p>Parcialmente (alguns dados pessoais tratados pela organização foram identificados).</p> <p>Não (a organização não identificou os dados pessoais que são tratados por ela).</p>	<p>Não (a organização não identificou os dados pessoais que são tratados por ela).</p>	<p>O plano de ação juntado ao PROAD 8737/2019 contempla, como um dos itens, o mapeamento de dados.</p> <p>A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização.</p> <p>Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.</p>
3.6.1 A organização identificou os locais onde os dados pessoais identificados são armazenados?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Parcialmente (alguns dados pessoais tratados pela organização foram identificados),' ou 'Sim (todos os dados pessoais tratados pela organização foram identificados),' na questão '13 [Q36]' (3.6 A organização identificou quais são os dados pessoais tratados por ela?)</p> <p>Referência(s): Lei 13.709/2018, art. 5º, inciso I; art. 37. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.1 e 7.2.8.</p> <p>Os dados pessoais podem ser armazenados em ativos de TI (e.g.: servidor de arquivos, nuvem, dispositivo USB, storage, fita de backup) ou em arquivos físicos (e.g.: pastas e armários). As organizações também devem identificar o local (endereço) onde se encontram os dados.</p>	<p>Sim (a organização identificou os locais onde são armazenados todos os dados pessoais que já foram identificados).</p> <p>Parcialmente (a organização identificou os locais onde são armazenados alguns dos dados pessoais que já foram identificados).</p> <p>Não (a organização não identificou os locais onde são armazenados os dados pessoais que já foram identificados).</p>	<p>Condicional a resposta anterior</p>	<p>O plano de ação juntado ao PROAD 8737/2019 contempla, como um dos itens, o mapeamento de dados.</p> <p>A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização.</p> <p>Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.</p> <p>Ainda assim, registre-se que sabemos onde a SETIC armazena os dados pessoais digitalizados e as ações técnicas e procedimentais para cuidar deles são realizadas.</p>



<p>3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?</p> <p>4. Liderança</p> <p>A alta direção deve demonstrar liderança e comprometimento com a iniciativa de adequação à LGPD.</p>	<p>Só responder essa pergunta sob as seguintes condições: A resposta foi "Parcialmente (alguns processos de negócio que realizam tratamento de dados pessoais foram identificados)," ou "Sim (todos os processos de negócio que realizam tratamento de dados pessoais foram identificados)," na questão "11 [Q35]" (3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?) e A resposta foi "Sim (todos os dados pessoais tratados pela organização foram identificados)," ou "Parcialmente (alguns dados pessoais tratados pela organização foram identificados)," na questão "13 [Q36]" (3.6 A organização identificou quais são os dados pessoais tratados por ela?)</p> <p>Critério(s): Lei 13.709/2018, art. 50, § 1º e § 2º, inciso I, alínea "d". ABNT NBR ISO/IEC 27.701/2019, item 5.4.1.2. A organização deve avaliar os riscos associados aos processos que realizam tratamento de dados pessoais. Essa avaliação auxilia a organização a compreender as consequências e as probabilidades dos riscos para direcionar a definição de quais processos devem ser priorizados na iniciativa de adequação à LGPD.</p>	<p>Sim Não</p>	<p>Não</p>	<p>O plano de ação juntado ao PROAD 8737/2019 contempla, como um dos itens, o mapeamento de dados.</p> <p>A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização.</p> <p>Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.</p>
<p>4.1 A organização possui Política de Segurança da Informação ou instrumento similar?</p>	<p>Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, itens 5.3.2 e 6.2.</p> <p>Uma Política de Segurança da Informação estabelece a abordagem da organização para gerenciar os objetivos de segurança da informação. A referida política deve ser aprovada pela alta direção e estar de acordo com os requisitos de negócio e com leis e regulamentações aplicáveis.</p>	<p>Sim Não</p>	<p>Sim</p>	<p>Existe e vai ser atualizada pela SETIC com o Plano de Ação decorrente das Res. 360, 361 e 362?</p> <p>http://trtapl3.trt12.gov.br/cmdg/img_legis/2018/042711149.pdf</p> <p>Confirmar se a SETIC atualizou a Política antes de enviar o formulário.</p>
<p>4.1.1 Anexe a Política de Segurança da Informação (ou instrumento similar) da organização:</p>	<p>Só responder essa pergunta sob as seguintes condições: A resposta foi "Sim" na questão "16 [Q41]" (4.1 A organização possui Política de Segurança da Informação ou instrumento similar?)</p>	<p>Carregar arquivo comprovando. (Só se aceite o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)</p>	<p>Sim</p>	<p>Confirmar se o arquivo que está no site é o correto (atualização)</p> <p>http://trtapl3.trt12.gov.br/cmdg/img_legis/2018/042711149.pdf</p>
<p>4.2 A organização possui Política de Classificação da Informação ou instrumento similar?</p>	<p>Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.</p> <p>Uma Política de Classificação da Informação deve fornecer diretrizes para assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.</p>	<p>Sim Não</p>	<p>Não</p>	<p>Por ora, não faremos ação.</p>
<p>4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?</p>	<p>Só responder essa pergunta sob as seguintes condições: A resposta foi "Sim" na questão "18 [Q42]" (4.2 A organização possui Política de Classificação da Informação ou instrumento similar?)</p> <p>Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.</p> <p>A Política de Classificação da Informação deve considerar a classificação de dados pessoais para viabilizar a identificação de quais desses dados são tratados pela organização, o que é importante para direcionar a implementação de controles adequados para a proteção de dados pessoais.</p>	<p>Sim Não</p>	<p>Condicional a 4.2</p>	<p></p>
<p>4.2.1.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?</p>	<p>Só responder essa pergunta sob as seguintes condições: A resposta foi "Sim" na questão "19 [Q421]" (4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?)</p> <p>Referência(s): Lei 13.709/2018, art. 5º, inciso II; art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.2.</p> <p>O dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. A LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais sensíveis.</p>	<p>Sim Não</p>	<p>Condicional a 4.2</p>	<p></p>
<p>4.2.1.2 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?</p>	<p>Só responder essa pergunta sob as seguintes condições: A resposta foi "Sim" na questão "19 [Q421]" (4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?)</p> <p>Referência(s): Lei 13.709/2018, art. 14; art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.2.</p> <p>A LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais de crianças e de adolescentes.</p>	<p>Sim Não</p>	<p>Condicional a 4.2</p>	<p></p>



4.2.2 Anexe a Política de Classificação da Informação (ou instrumento similar) da organização:	Só responder essa pergunta sob as seguintes condições: A resposta foi 'Sim' na questão '18 [Q42]' (4.2 A organização possui Política de Classificação da Informação ou instrumento similar?)	Carregar arquivo comprovando. (Só é aceito o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)	Não temos.	
4.3 A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?	Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, itens 6.2.1. A Política de Proteção de Dados Pessoais deve estar alinhada com a Política de Segurança da Informação e com a Política de Classificação da Informação e prevê apoio e comprometimento da organização para alcançar a conformidade com os normativos de proteção de dados pessoais. A Política de Proteção de Dados Pessoais pode ser definida e publicada em documento específico ou incluída no texto da Política de Segurança da Informação já existente. Vale ressaltar que a Política de Proteção de Dados Pessoais não se confunde com a Política de Privacidade. Enquanto a primeira é voltada para o público interno da organização, a segunda é direcionada para o público externo (e.g.: titulares de dados pessoais).	Sim Não	Não.	A política de proteção de dados do Tribunal está em vias de revisão para contemplar os Dados Pessoais. Política de Segurança atual: http://trtap3.trt12.gov.br/cmdg/img_legis/2018/042711149.pdf A ação integra as ações da TI no Plano de Ação do PROAD 8737/2019.
4.3.1 Anexe a Política de Proteção de Dados Pessoais (ou documento similar) da organização:	Só responder essa pergunta sob as seguintes condições: A resposta foi 'Sim' na questão '23 [Q43]' (4.3 A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?)	Carregar arquivo comprovando. (Só é aceito o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)	Condicional a anterior	
4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?	Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1. O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O termo DPO (Data Protection Officer) é comumente utilizado para se referir ao encarregado. Convém que o encarregado possua, além de profundo conhecimento da Lei 13.709/2018, conhecimentos relativos a temas como: Direito, Governança Corporativa, Gestão de Riscos, Tecnologia da Informação e Segurança da Informação.	Sim Não	Sim	Juiz Roberto Masami Nakajo (Portaria PRESI nº 15, de 26 de janeiro de 2021) Disponibilização: 25-2-2021 Publicação: 26-2-2021 - DEJT
4.4.1 A nomeação do encarregado foi publicada em veículo de comunicação oficial?	Só responder essa pergunta sob as seguintes condições: A resposta foi 'Sim' na questão '25 [Q44]' (4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?) Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 2º. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1. A organização deve designar oficialmente o encarregado. Diante disso, é conveniente que a nomeação do encarregado seja publicada em veículo de comunicação oficial como o Diário Oficial da União (DOU).	Sim Não	Sim	Juiz Roberto Masami Nakajo (Portaria PRESI nº 15, de 26 de janeiro de 2021) Disponibilização: 25-2-2021 Publicação: 26-2-2021 - DEJT
4.4.2 Em qual setor da organização está lotado o encarregado?	Só responder essa pergunta sob as seguintes condições: A resposta foi 'Sim' na questão '25 [Q44]' (4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?) Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 1º, § 1º, inciso II. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1. O encarregado deve ser independente e ter liberdade para reportar à alta administração. É recomendável que o encarregado não faça parte de um setor no qual possa haver conflito de interesses.	Tecnologia da Informação Jurídico Ouidoria Auditoria/Controle Interno (compliance) Outros	Jurídico	Juiz Roberto Masami Nakajo (Portaria PRESI nº 15, de 26 de janeiro de 2021) Disponibilização: 25-2-2021 Publicação: 26-2-2021 - DEJT
4.4.3 A identidade e as informações de contato do encarregado foram divulgadas na internet?	Só responder essa pergunta sob as seguintes condições: A resposta foi 'Sim' na questão '25 [Q44]' (4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?) Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41, § 1º. IN SGD/ME 117/2020, art 2º. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1. A identidade e as informações de contato (e.g.: e-mail, telefone) do encarregado devem ser divulgadas publicamente, preferencialmente no sítio eletrônico da organização.	Sim Não	Sim	https://portal.trt12.jus.br/lcpd/encarregado-pelo-tratamento-de-dados-pessoais
5. Capacitação A organização deve conduzir iniciativas para conscientizar e capacitar os colaboradores em proteção de dados pessoais.				



5.1 A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?	<p>Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.</p> <p>É conveniente que a organização elabore um Plano de Capacitação que determine as competências necessárias para os recursos humanos envolvidos em atividades que realizam o tratamento de dados pessoais. O Plano de Capacitação deve mapear as lacunas de conhecimento associadas ao tema, bem como planejar ações de treinamento para redução dessas lacunas.</p> <p>Ademais, é necessário que todas as pessoas da organização estejam cientes da importância do tema proteção de dados pessoais e dos impactos que podem ser causados devido à violação desses dados. Diante disso, é importante que o plano de capacitação também contemple ações de conscientização.</p> <p>Nada impede que a organização elabore um plano de conscientização apartado de um plano de treinamento.</p>	<p>Sim</p> <p>Não</p>		<p>Verificar validação e aprovação até o dia 30-3.</p>
5.1.1 O Plano de Capacitação (ou instrumento similar) considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '29 [Q51]' (5.1 A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?)</p> <p>Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.</p> <p>Por exemplo, recursos humanos envolvidos em atividades críticas relacionadas ao tratamento de dados pessoais devem receber treinamento além do nível básico fornecido aos demais colaboradores.</p>	<p>Sim</p> <p>Não</p>	<p>Não</p>	<p>Nesse momento o Plano não considerará as diversas funções - isso será feito a medida que houver o amadurecimento da Instituição com a execução do Plano de Ação.</p>
5.1.2 Anexa o Plano de Capacitação (ou instrumento similar) da organização:	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '29 [Q51]' (5.1 A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?)</p>	<p>Carregar arquivo comprovando.</p> <p>(Só é aceito o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)</p>		<p>Juntar arquivo aprovado no PROAD 8737/2019.</p>
5.2. Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?	<p>Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.</p> <p>Diante da vigência da LGPD, é conveniente que os colaboradores envolvidos diretamente em atividades que realizam o tratamento de dados pessoais já tenham participado de treinamentos correlatos ao tema</p>	<p>Sim (todos os colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema).</p> <p>Parcialmente (alguns colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema).</p> <p>Não (nenhum dos colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema).</p>	<p>Parcialmente (alguns colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema).</p>	<p>Considerou-se para a resposta todos os servidores do Tribunal.</p> <p>Até o momento da resposta ao TCU foi realizada capacitação pela Escola Judicial (UFSC - 2020) e disponibilizado curso pela plataforma EDUCERE (SEDUC).</p>
<p>6. Conformidade do tratamento</p> <p>A organização deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos. Para isso é fundamental demonstrar que os princípios estabelecidos pela LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.</p>				
6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?	<p>Referência(s): Lei 13.709/2018, art. 6º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 7.2.1.</p> <p>As atividades de tratamento de dados pessoais devem ter propósitos legítimos, específicos, explícitos e informados ao titular.</p> <p>A organização deve assegurar que os titulares de dados pessoais entendam a(s) finalidade(s) pelas quais os seus dados pessoais são tratados</p>	<p>Sim (todas as finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas).</p> <p>Parcialmente (algumas finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas).</p> <p>Não (as finalidades das atividades de tratamento de dados pessoais ainda não foram identificadas e documentadas).</p>	<p>Não (as finalidades das atividades de tratamento de dados pessoais ainda não foram identificadas e documentadas).</p>	<p>O plano de ação contempla, como um dos itens, o mapeamento de dados, que contemplará identificação e documentará as finalidades das atividades de tratamento de dados pessoais.</p> <p>A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização.</p> <p>Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.</p>
6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' (todas as finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas), ou 'Parcialmente' (algumas finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas), na questão '33 [Q61]' (6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?)</p> <p>Referência(s): Lei 13.709/2018, art. 6º, incisos II e III. ABNT NBR ISO/IEC 27.701/2019, item 7.4.1.</p> <p>Os dados pessoais coletados devem se limitar ao que é estritamente necessário para cumprir com as finalidades de tratamento.</p>	<p>Sim</p> <p>Não</p>	<p>Vinculado ao 6.1.</p>	<p>Isso foi feito apenas no Plano de Ações dos contratos - mas é um universo mínimo de dados frente ao total.</p>



6.1.2 A organização avaliou se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim (todas as finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas).' ou 'Parcialmente (algumas finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas).' na questão '33 [Q61]' (6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?)</p> <p>Referência(s): Lei 13.709/2018, art. 40. ABNT NBR ISO/IEC 27.701/2019, item 7.4.7.</p> <p>A organização não deve reter dados pessoais por tempo maior do que o estritamente necessário.</p>	<p>Sim</p> <p>Não</p>	<p>Vinculado ao 6.1.</p>	<p>Isso foi feito apenas no Plano de Ações dos contratos - mas é um universo mínimo de dados frente ao total.</p>
6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?	<p>Referência(s): Lei 13.709/2018 art. 7º. ABNT NBR ISO/IEC 27.701/2019, item 7.2.2.</p> <p>A organização deve determinar e documentar as bases legais que fundamentam as atividades de tratamento de dados pessoais. As bases legais são relacionadas no art. 7º da Lei 13.709/2018: consentimento; cumprimento de obrigação legal ou regulatória; execução de políticas públicas pela Administração Pública; estudos por órgão de pesquisa; execução de contrato; exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física; tutela da saúde; interesse legítimo; e proteção do crédito.</p>	<p>Sim (as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização foram definidas e documentadas).</p> <p>Parcialmente (as bases legais que fundamentam algumas das atividades de tratamento de dados pessoais da organização foram definidas e documentadas).</p> <p>Não (nenhuma base legal que fundamenta as atividades de tratamento de dados pessoais da organização foi definida e documentada).</p>	<p>Não (nenhuma base legal que fundamenta as atividades de tratamento de dados pessoais da organização foi definida e documentada).</p>	<p>O plano de ação contempla, como um dos itens, o mapeamento de dados, que contemplará identificação e documentará as bases legais que fundamentam as atividades de tratamento de dados pessoais.</p> <p>A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização.</p> <p>Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.</p>
6.3 Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?	<p>Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.</p> <p>Uma maneira de reter os registros das características das atividades de tratamento de dados pessoais é por meio de um inventário, o qual pode contemplar, por exemplo: finalidade do tratamento; base legal que fundamenta o tratamento; descrição das categorias dos titulares de dados pessoais envolvidos no tratamento; dados pessoais coletados; tempo de retenção dos dados; local de armazenamento dos dados; responsável pelo processo de tratamento; e medidas de segurança adotadas.</p>	<p>Sim</p> <p>Não</p>	<p>Não</p>	<p>O plano de ação contempla, como um dos itens, o mapeamento e inventário de dados (este como resultado do mapeamento).</p> <p>A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização.</p> <p>Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação.</p>
6.3.1 Anexe o arquivo que representa o registro das atividades de tratamento de dados pessoais (e.g.: inventário):	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '37 [Q63]' (6.3 Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?)</p>	<p>Carregar arquivo.</p> <p>(Só é aceito o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)</p>	<p>Vinculado ao 6.3.</p>	
6.4 A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?	<p>Referência(s): Lei 13.709/2018, art. 5º, inciso XVII; art. 38. ABNT NBR ISO/IEC 27.701/2019, item 7.2.5.</p> <p>O Relatório de Impacto à Proteção de Dados Pessoais é uma documentação do controlador que contempla a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos titulares e das medidas adotadas para tratamento desses riscos.</p> <p>O relatório deve 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 da organização quanto às medidas, salvaguardas e mecanismos de mitigação de riscos.</p> <p>Só responder essa pergunta sob as seguintes condições:</p>	<p>Sim (a organização elaborou Relatório de Impacto à Proteção de Dados Pessoais que abrange TODOS os processos de tratamento de dados pessoais que podem gerar riscos aos titulares).</p> <p>Sim (a organização elaborou Relatório de Impacto à Proteção de Dados Pessoais que abrange ALGUNS processos de tratamento de dados pessoais que podem gerar riscos aos titulares).</p> <p>Não.</p> <p>Não se aplica (a organização não executa processo de tratamento de dados pessoais que pode gerar riscos às liberdades civis e aos direitos fundamentais dos titulares).</p>	<p>Não.</p>	<p>A ação está prevista no Plano da SETIC para adequação à LGPD.</p>
6.4.1 A organização implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais?	<p>A resposta foi 'Sim (a organização elaborou Relatório de Impacto à Proteção de Dados Pessoais que abrange TODOS os processos de tratamento de dados pessoais que podem gerar riscos aos titulares).' ou 'Sim (a organização elaborou Relatório de Impacto à Proteção de Dados Pessoais que abrange ALGUNS processos de tratamento de dados pessoais que podem gerar riscos aos titulares).' na questão '39 [Q64]' (6.4 A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?)</p> <p>Referência(s): Lei 13.709/2018, art. 5º, inciso XVII; art. 38. ABNT NBR ISO/IEC 27.701/2019, item 7.2.5.</p> <p>A organização deve adotar medidas para tratar os riscos identificados por meio da avaliação de impacto sobre a proteção de dados pessoais.</p>	<p>Sim (a organização implementou controles para mitigar todos os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais).</p> <p>Parcialmente (a organização implementou controles para mitigar alguns riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais).</p> <p>Não (a organização não implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais).</p>	<p>Condicional ao item anterior.</p>	<p>A ação está prevista no Plano da SETIC para adequação à LGPD.</p>
<p>7. Direitos do titular</p> <p>A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais. Para isso, a organização deve publicar, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais. A organização também deve estar preparada para atender todos os direitos dos titulares que</p>				



7.1 A organização possui Política de Privacidade (ou instrumento similar)?	<p>Referência(s): Lei 13.709/2018, art. 6º, inciso VI; art. 9º; art. 23, inciso I; art. 50, inciso I, alíneas "a", "d" e "e". ABNT NBR ISO/IEC 27.701/2019, itens 7.3.2 e 7.3.3.</p> <p>A Política de Privacidade deve documentar e comunicar aos titulares de dados pessoais, de maneira clara e concisa, informações relativas ao tratamento de seus dados pessoais.</p> <p>A LGPD exemplifica informações que devem constar no referido artefato: as finalidades dos tratamentos; as formas e as durações dos tratamentos; a identificação e os dados de contato do controlador; as informações acerca do uso compartilhado de dados; as responsabilidades dos agentes que realizam os tratamentos; e os direitos do titular.</p> <p>Além disso, o Poder Público deve informar as hipóteses em que, no exercício de suas competências, realiza tratamento de dados pessoais, fornecendo informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.</p> <p>O termo "Aviso de Privacidade" é comumente utilizado para se referir à Política de Privacidade.</p>	Sim Não	Sim	https://portal.trt12.jus.br/igpd/politica-de-privacidade/
7.1.1 A Política de Privacidade (ou instrumento similar) está publicada na internet?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '41 [Q71]' (7.1 A organização possui Política de Privacidade (ou instrumento similar)?)</p> <p>Referência(s): Lei 13.709/2018, art. 6º, inciso VI; art. 9º; art. 50, inciso I, alínea "e". ABNT NBR ISO/IEC 27.701/2019, item 7.3.3.</p> <p>A Política de Privacidade deve ser publicada em local facilmente acessível pelos titulares de dados pessoais. Além de fornecer acesso à política no momento da coleta dos dados pessoais, convém que a organização forneça acesso ao artefato de forma permanente no sítio institucional.</p>	Sim Não	Sim	https://portal.trt12.jus.br/igpd/politica-de-privacidade/
7.1.1.1 Favor informar o endereço da internet (URL) onde a política está publicada:	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '42 [Q711]' (7.1.1 A Política de Privacidade (ou instrumento similar) está publicada na internet?)</p>	Inserir link.	https://portal.trt12.jus.br/igpd/politica-de-privacidade/	
7.1.2 Anexa a Política de Privacidade (ou instrumento similar) da organização:	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '42 [Q711]' (7.1.1 A Política de Privacidade (ou instrumento similar) está publicada na internet?)</p>	Carregar arquivo. (Só é aceito o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)	https://portal.trt12.jus.br/igpd/politica-de-privacidade/	Baixar o documento
7.2 Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?	<p>Referência(s): Lei 13.709/2018, art. 17-22. ABNT NBR ISO/IEC 27.701/2019, item 7.3.</p> <p>Quando aplicável, a organização deve atender aos direitos dos titulares estabelecidos no art. 18 da LGPD como, por exemplo: confirmação da existência de tratamento; acesso aos dados; e correção de dados.</p>	Sim (foram implementados mecanismos para atender todos os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização). Parcialmente (foram implementados mecanismos para atender alguns direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização). Não (não foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD).	Sim (foram implementados mecanismos para atender todos os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização).	https://portal.trt12.jus.br/igpd/direitos-do-titular/
8. Compartilhamento de dados pessoais A organização deve documentar detalhes relacionados ao compartilhamento de dados pessoais com terceiros.				
8.1 A organização identificou os dados pessoais são compartilhados com terceiros?	<p>Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.3 e 7.5.4.</p> <p>É conveniente que a organização tenha documentado quais os dados pessoais que são compartilhados com terceiros.</p>	Sim (os dados pessoais que são compartilhados com terceiros foram identificados). Parcialmente (alguns dados pessoais que são compartilhados com terceiros foram identificados). Não (não houve iniciativa para identificar dados pessoais que são compartilhados com terceiros). Não se aplica (a organização não realiza compartilhamento de dados pessoais com terceiros).	Não (não houve iniciativa para identificar dados pessoais que são compartilhados com terceiros).	O plano de ação contempla, como um dos itens, o mapeamento e nesse momento será verificada a existência de dados compartilhados. A Res. 363/2021 do CNJ prevê a realização do mapeamento, mas que será disponibilizado formulário para sua realização. Até o momento não foi fornecido o formulário pelo CNJ e o Tribunal ainda não iniciou a identificação."



8.1.1 Os compartilhamentos de dados pessoais identificados estão em conformidade com os critérios estabelecidos na LGPD?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim (os dados pessoais que são compartilhados com terceiros foram identificados),' ou 'Parcialmente (alguns dados pessoais que são compartilhados com terceiros foram identificados),' na questão '46 [Q81]' (8.1 A organização identificou os dados pessoais são compartilhados com terceiros?)</p> <p>Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.3 e 7.5.4.</p> <p>Os compartilhamentos de dados pessoais devem respeitar os critérios estabelecidos na LGPD. Diante disso, os casos de compartilhamento devem ser avaliados para que sejam efetuados os devidos ajustes.</p> <p>O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal e respeitar os princípios elencados no art. 6º da LGPD.</p> <p>Ademais, há a necessidade de que os contratos e convênios que impliquem uso compartilhado, transferência ou comunicação de dados pessoais com entidades privadas sejam objeto de comunicação à ANPD.</p>	<p>Sim (os compartilhamentos de dados pessoais estão em conformidade com os critérios estabelecidos na LGPD).</p> <p>Parcialmente (alguns compartilhamentos de dados pessoais estão em conformidade com os critérios estabelecidos na LGPD).</p> <p>Não (os compartilhamentos de dados pessoais não estão em conformidade com os critérios estabelecidos na LGPD).</p>	Vinculado ao 8.1	
8.1.2 A organização registra eventos relacionados à transferência dos dados pessoais que são compartilhados com terceiros e que foram identificados?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim (os dados pessoais que são compartilhados com terceiros foram identificados),' ou 'Parcialmente (alguns dados pessoais que são compartilhados com terceiros foram identificados),' na questão '46 [Q81]' (8.1 A organização identificou os dados pessoais são compartilhados com terceiros?)</p> <p>Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.4.</p> <p>É conveniente que a organização tenha registros de quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados.</p>	<p>Sim (a organização registra eventos relacionados à transferência de todos os dados pessoais que são compartilhados com terceiros e que foram identificados).</p> <p>Parcialmente (a organização registra eventos relacionados à transferência de alguns dados pessoais que são compartilhados com terceiros e que foram identificados).</p> <p>Não (a organização não registra eventos relacionados à transferência dos dados pessoais que são compartilhados com terceiros e que foram identificados).</p>	Vinculado ao 8.1	
8.1.3 Algum caso de compartilhamento envolve transferência internacional de dados pessoais?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Parcialmente (alguns dados pessoais que são compartilhados com terceiros foram identificados),' ou 'Sim (os dados pessoais que são compartilhados com terceiros foram identificados),' na questão '46 [Q81]' (8.1 A organização identificou os dados pessoais são compartilhados com terceiros?)</p> <p>Referência(s): Lei 13.709/2018, arts 33-36. ABNT NBR ISO/IEC 27.701/2019, item 7.5.1 e 7.5.2.</p> <p>A LGPD relaciona os casos nos quais é permitida a transferência internacional de dados pessoais. Diante disso, é conveniente que a organização identifique os casos em que isso ocorre para avaliar se estão em conformidade com as hipóteses estabelecidas na lei.</p>	<p>Sim</p> <p>Não</p> <p>A organização ainda não verificou se há caso de compartilhamento que envolva transferência internacional de dados pessoais.</p>	Vinculado ao 8.1	
8.1.3.1 As transferências internacionais de dados pessoais estão de acordo com os casos previstos na LGPD?	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '49 [Q813]' (8.1.3 Algum caso de compartilhamento envolve transferência internacional de dados pessoais?)</p> <p>Referência(s): Lei 13.709/2018, arts. 33-36. ABNT NBR ISO/IEC 27.701/2019, item 7.5.2.</p> <p>A organização deve avaliar se a transferência internacional de dados pessoais se enquadra em um dos casos previstos no art. 33 da LGPD.</p>	<p>Sim</p> <p>Não</p>	Vinculado ao 8.1.3	
9. Violação de dados pessoais				
A organização deve gerenciar incidentes de segurança da informação que envolvem a violação de dados pessoais.				
9.1 A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais?	<p>Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.1.</p> <p>Como parte do processo de gestão de incidentes de segurança da informação global, é conveniente que a organização estabeleça responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes que envolvem violação de dados pessoais.</p>	<p>Sim</p> <p>Não</p>	Sim	Em fase de revisão - conforme Plano de Ação para adequação às Resoluções CNJ 360 a 363.
9.1.1 Anexe o Plano de Resposta a Incidentes (ou documento similar) da organização:	<p>Só responder essa pergunta sob as seguintes condições:</p> <p>A resposta foi 'Sim' na questão '51 [Q81]' (9.1 A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais?)</p>	<p>Carregar arquivo.</p> <p>(Só é aceito o upload de um único arquivo no formato PDF, com tamanho máximo de 20MB.)</p>		Anexar documento válido no momento da resposta com a SETIC.
9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?	<p>Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.1.</p> <p>Convém que a organização possua um sistema de informação de gestão de incidentes que viabiliza o tratamento de casos que envolvem violação de dados pessoais. Essa gestão inclui o registro dos incidentes.</p>	<p>Sim</p> <p>Não</p>	Sim	CSI - Assyst



9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?	Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.5. Convém que a organização possua sistema para o registro das ações adotadas para solucionar os incidentes que envolvem violação de dados pessoais. O tratamento de incidentes pode envolver, primeiramente, a adoção de solução de contorno para, posteriormente, haver análise e erradicação da causa.	Sim Não	Sim	CSI - Assyst
9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?	Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, itens 6.13.1.4 e 6.13.1.5. Convém que a organização adote mecanismo para monitorar proativamente os eventos de segurança da informação que são associados à violação de dados pessoais para adotar medidas necessárias caso ocorram. A identificação precoce de incidentes pode diminuir significativamente os impactos causados por eles.	Sim Não	Não	A resposta seria "parcialmente", uma vez que nem tudo está automatizado. O monitoramento pelo sistema é realizado 24/7, mas o tratamento pelos servidores (resposta) ocorre apenas dentro do horário de expediente. Não há sobreaviso e plantão para equipe de segurança da informação.
9.5 A organização estabeleceu procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?	Referência(s): Lei 13.709/2018, art. 48. ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.5. A organização deve comunicar à ANPD e ao titular a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares. A notificação deve ser feita em prazo razoável e mencionar, no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança adotadas para a proteção dos dados; os riscos relacionados ao incidente; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Caso a organização não encaminhe a comunicação tempestivamente, deverá ser exposto, também, os motivos que levaram à demora.	Sim Não	Sim	Portaria Conjunta 14/2021. Será previsto expressamente na Política de Segurança da Informação.
10. Medidas de proteção				
A organização deve adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais. Para isso, convém que sejam implementados controles capazes de mitigar riscos que possam resultar em violação da privacidade.				
10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?	Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.002/2013, item 6.1. A organização deve adotar medidas de segurança, técnicas e administrativas, aptas a 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.	Sim Não	Sim	Sim, temos vários mecanismos, políticas e procedimentos para proteger os dados, incluindo a política de backup
10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?	Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.701/2019, itens 6.6.2.1 e 6.6.2.2. Convém que a organização defina processo formal para registro e cancelamento de usuários para viabilizar a atribuição dos direitos de acesso aos sistemas que realizam tratamento de dados pessoais. O mesmo deve ser feito com o processo de provisionamento para conceder ou revogar os direitos de acesso dos usuários nesses sistemas. Convém que a concessão de direitos de acesso observem os princípios de "necessidade de conhecer" e "necessidade de uso".	Sim (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em todos os sistemas que realizam tratamento de dados pessoais). Parcialmente (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em alguns sistemas que realizam tratamento de dados pessoais). Não (a organização não implementou processo formal para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais).		SETIC verificará essa questão.
10.3 A organização registra eventos das atividades de tratamento de dados pessoais?	Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.701/2019, item 6.9.4.1. Convém que a organização registre os eventos (logs) das atividades de tratamento de dados pessoais de forma que seja possível identificar por quem, quando e quais dados pessoais foram acessados. Nos casos em que ocorrem mudanças nos dados, também deve ser registrada a ação realizada (e.g.: inclusão, alteração ou exclusão).	Sim (a organização registra os eventos de todas as atividades de tratamento de dados pessoais). Parcialmente (a organização registra os eventos de algumas atividades de tratamento de dados pessoais). Não (a organização não registra os eventos de atividades de tratamento de dados pessoais).	Parcialmente (a organização registra os eventos de algumas atividades de tratamento de dados pessoais).	Alterações no F: são alterados. Pje são controlados. Nossa resposta é "parcialmente" porque no SIGEP e no PROAD fazemos o tratamento apenas na criação, alteração e exclusão dos dados. Não temos o controle de quem acessou os dados apenas para leitura. Conforme Nelson comentou, exceção ocorre no acesso externo ao PROAD (pelo Portal PROAD), onde é registrado também o acesso aos dados pelos usuários externos. Podemos apenas indicar que tanto no SIGEP quanto no PROAD registramos apenas a criação, alteração e exclusão de dados. Confirmei no sistema e o registro da consulta de dados, mesmo por usuários externos, é bastante limitada. Para usuários externos, por exemplo, apenas a primeira consulta ao documento é registrada.
10.4 A organização utiliza criptografia para proteger os dados pessoais?	Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alínea "c". ABNT NBR ISO/IEC 27.701/2019, item 6.7. A utilização de criptografia pode proteger a confidencialidade, a autenticidade e/ou a integridade da informação. Por exemplo, devido à criticidade dos dados sensíveis, a adoção de mecanismos para criptografá-los em trânsito e no armazenamento pode mitigar riscos associados à violação de dados pessoais.	Sim (a organização utiliza criptografia para proteger todos os dados pessoais). Parcialmente (a organização utiliza criptografia para proteger alguns dados pessoais). Não (a organização não utiliza criptografia para proteger os dados pessoais).	Não (a organização não utiliza criptografia para proteger os dados pessoais).	
10.5 A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (Privacy by Design e Privacy by Default)?	Referência(s): Lei 13.709/2018, art. 46, § 2º. ABNT NBR ISO/IEC 27.701/2019, item 7.4. A organização deve assegurar que os processos e sistemas sejam projetados de forma que os tratamentos de dados pessoais estejam limitados ao que é estritamente necessário para alcance da finalidade pretendida.	Sim Não		SETIC verificará essa questão.



Cell: A26

Comment: @valdir.cunha@trt12.jus.br @anderson.bastos@trt12.jus.br e @arthur.lago@trt12.jus.br - Os instrumentos da Segurança da Informação atenderiam esse item e seus subitens?
Atribuído a Valdir Cunha
-Direção Geral da Secretaria (DIGER)

Cell: A31

Comment: @valdir.cunha@trt12.jus.br @anderson.bastos@trt12.jus.br e @arthur.lago@trt12.jus.br

Está incluída na Política d e Segurança?
-Direção Geral da Secretaria (DIGER)

Cell: A51

Comment: @valdir.cunha@trt12.jus.br @arthur.lago@trt12.jus.br e @anderson.bastos@trt12.jus.br - seria o mesmo que a avaliação das vulnerabilidades ? (inciso II do art. 2º da Res. CNJ 363/2021.)
Atribuído a Valdir Cunha
-Direção Geral da Secretaria (DIGER)

Cell: A69

Comment: @valdir.cunha@trt12.jus.br @arthur.lago@trt12.jus.br e @anderson.bastos@trt12.jus.br . Checar o que seria necessário para atualizar até 30-3.
Atribuído a Valdir Cunha
-Direção Geral da Secretaria (DIGER)

Cell: A75

Comment: @valdir.cunha@trt12.jus.br @anderson.bastos@trt12.jus.br e @arthur.lago@trt12.jus.br - todos os subitens do 10 são SETIC/Segurança da Informação (pelo que analise).

Podem verificar?
Atribuído a Valdir Cunha
-Direção Geral da Secretaria (DIGER)

