

RELATÓRIO DO MAPEAMENTO DE PROCESSOS DE TRABALHO COM O TRATAMENTO DE DADOS PESSOAIS

O presente relatório tem por objetivo descrever o projeto de mapeamento de processos de trabalho onde há o tratamento de dados pessoais no Tribunal de Justiça de Santa Catarina, indicando as etapas executadas para alcançar-se o resultado e os achados desse trabalho.

A LGPD instituiu em seu artigo 19, inciso II, que o Controlador deverá informar aos titulares, a partir de solicitação de declaração completa, a inexistência de registro ou a origem dos dados pessoais tratados, os critérios utilizados e a finalidade do tratamento, em até 15 dias após a requisição. Neste contexto, o CGPDP previu, no conjunto de ações e projetos para a implementação da LGPD no PJSC, a realização de mapeamento dos dados pessoais através da aplicação de formulário específico para levantamento de informações junto aos órgãos que fazem parte da administração desta Corte (item 2.8. do *Roadmap*).

A Resolução n. 363/2021 do CNJ, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais, ratificou esta necessidade no seu artigo 1º, inciso 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”.

1. PROJETO

O trabalho teve início em fevereiro de 2021, com os estudos sobre a matriz de mapeamento que seria utilizada para o levantamento das informações pretendidas nas áreas administrativas do TJSC. Após a verificação de diversos modelos disponíveis no mercado e aplicados por outros órgãos, chegou-se à conclusão que nenhum deles era aplicável ao TJSC, para o conjunto de informações que se pretendia obter e com o detalhamento esperado.

Nesse contexto, decidiu-se pela elaboração de uma matriz própria de mapeamento de processos com dados pessoais, que fosse fácil de compreender, privilegiasse a facilidade no preenchimento, contemplasse todos os aspectos exigidos pela LGPD e considerasse o nível de maturidade do TJSC em relação ao tema, observado no questionário sobre a LGPD aplicado em todo o Poder Judiciário de Santa Catarina no período de setembro a novembro de 2020.

A incumbência de desenhar uma matriz de mapeamento e conduzir os trabalhos junto às unidades objeto do levantamento foi repassada ao Grupo de Trabalho para a Implementação da LGPD, vinculado ao CGPDP.

1.1 Matriz de Mapeamento

A matriz elaborada para a realização do mapeamento é baseada numa planilha do software Excel, a qual possui um cabeçalho para identificação do setor onde está sendo efetuado o levantamento e do responsável pelo preenchimento das informações, além de 21 questões para serem respondidas sobre os processos com o tratamento de dados pessoais identificados.

As questões estão divididas em 8 grupos, identificados por cores distintas na planilha, conforme segue:

IDENTIFICAÇÃO DO PROCESSO

1. Nome do processo de trabalho em que há o tratamento de dados pessoais

2. Descrição sucinta do processo de trabalho
3. Setor responsável pelo processo de trabalho

FINALIDADE E BASE LEGAL

4. Finalidade do processo de trabalho
5. Base legal para tratamento dos dados pessoais do processo

DADOS PESSOAIS TRATADOS

6.1 a 6.11: Nome, RG, CPF, E-mail, Endereço, Telefone, Filiação, Estado Civil, Cargo ou Profissão, Reg. Profissional, Outros dados pessoais

DADOS PESSOAIS SENSÍVEIS TRATADOS

7.1 a 7.8: Origem racial / étnica, Convicção religiosa, Opinião política, Filiação a organização, Saúde ou vida sexual, Genético ou biométrico, Documento com foto, Outros dados pessoais sensíveis.

ORIGEM E ARMAZENAMENTO DOS DADOS

8. Origem da coleta dos dados
9. Tipo dos dados
10. Nome do sistema ou local onde os dados são armazenados
11. Período de tempo de retenção dos dados

SEGURANÇA DA INFORMAÇÃO

12. Os dados deste processo são anonimizados ou criptografados?
13. Há política para mitigar os efeitos de incidentes de segurança?
14. Há política para remediar os efeitos de algum incidente de segurança?

ACESSO E COMPARTILHAMENTO

15. Os dados deste processo são tratados em outro país?
16. É feito algum controle de acesso aos dados deste processo?
17. Os dados deste processo são acessados por outras áreas do TJ?
18. Os dados deste processo são compartilhados com instituições governamentais externas?
19. Os dados deste processo são compartilhados com outras instituições externas?
20. O titular pode consultar os seus dados pessoais deste processo?

OBSERVAÇÕES

21. Observações / pontos não abordados / sugestões

Grande parte das questões possui campos predefinidos para seleção, de modo que o preenchimento torna-se facilitado ao usuário.

1.2 Metodologia para levantamento de informações

Para a realização do mapeamento em cada unidade administrativa, foram previstas as seguintes etapas:

- Identificar pessoa de referência na unidade;
- Relacionar os setores para mapeamento
- Realizar reunião de preparação da diretoria
- Preencher planilha de mapeamento
- Apresentar levantamento efetuado ao grupo de trabalho do mapeamento
- Realizar ajustes na planilha
- Encaminhar resultado final do mapeamento ao CGPDP

Foi realizado o preenchimento de uma planilha onde devem ser informados os processos de trabalho internos, os dados pessoais e os dados pessoais sensíveis tratados nesses processos, sua origem, classificação, base legal para tratamento, características de retenção, possíveis compartilhamentos e medidas de segurança adotados para sua proteção.

Identificar multiplicadores nas diretorias para auxiliar na orientação interna durante o levantamento de informações e servir de referência para a equipe do Grupo de Trabalho no mapeamento, identificando os responsáveis pelos processos, agendando as reuniões da diretoria, e auxiliando nos trabalhos com outras diretorias, quando possível.

1.3 Piloto

Para validação da metodologia estabelecida e da planilha a ser preenchida, foi realizado um mapeamento em caráter experimental na Diretoria de Material e Patrimônio na primeira quinzena de março. No preenchimento da matriz de mapeamento foi confirmada a facilidade de preenchimento da planilha e identificados pontos para ajuste, visando tornar mais claras algumas questões.

Informações importantes para o aperfeiçoamento do trabalho de mapeamento.

A definição de uma pessoa de referência, denominada “multiplicador”, mostrou-se de grande importância para a organização do trabalho interno de levantamento de informações, pelo seu conhecimento dos setores e dos processos internos da unidade objeto do levantamento, facilitando a comunicação interna e a organização para o preenchimento da planilha. Além disso, a presença de uma pessoa de referência auxiliou no repasse de diretrizes do CGPDP aos setores e também na eliminação de dúvidas com o grupo de trabalho e sua disseminação internamente no setor.

A matriz de mapeamento ajustada e a metodologia estabelecida foram apresentadas ao CGPDP em reunião realizada em 5/4/21, restando aprovadas para aplicação subsequente nas unidades administrativas do TJSC.

2. EXECUÇÃO

A metodologia estabelecida para o mapeamento nas unidades administrativas previu a realização de uma reunião individualizada com os envolvidos de cada diretoria, conduzida pela Desembargadora Coordenadora do CGPDP, onde eram repassados conceitos relacionados à LGPD, a justificativa do trabalho e informações básicas, além da realização de uma simulação de preenchimento da planilha, com um processo de trabalho da unidade. Dessa forma, foi elaborado um cronograma com o início dos trabalhos em dias distintos para cada unidade administrativa,

sendo que o prazo estabelecido para cada unidade administrativa finalizar o mapeamento foi de 10 dias úteis.

Para preparação da unidade para o início do mapeamento, o grupo de trabalho encaminhou e-mail (modelo em anexo), com a matriz de mapeamento em anexo, convidando para a reunião de apresentação da planilha e apresentando esclarecimentos sobre o desenvolvimento dos trabalhos.

O mapeamento foi dividido em 2 grandes grupos: o primeiro com as diretorias do TJSC e o segundo com os setores vinculados aos órgãos da cúpula da Corte. O trabalho se desenvolveu no período de **abril a agosto de 2021** e, durante esse período, foram realizadas 19 reuniões de abertura dos trabalhos, com algumas unidades agrupadas, atingindo todos os setores objeto do mapeamento.

Os integrantes do Grupo de Trabalho permaneceram à disposição das unidades para repassar orientações, dirimir dúvidas e auxiliar no preenchimento da planilha. Nos 5 meses de realização dos trabalhos foram realizadas reuniões operacionais com os multiplicadores das unidades e prestados mais de 140 atendimentos por telefone, Whatsapp e e-mail.

2.1 Mapeamento nas Diretorias

Inicialmente a matriz foi aplicada nas diretorias vinculadas às Direções-Gerais Administrativa (DGA) e Judiciária (DGJ) e Presidência, alcançando todas as **13 diretorias** do TJSC, suas divisões e seções, totalizando mais de **186 setores**, com processos de trabalho analisados e mapeados.

O mapeamento nas diretorias respeitou a seguinte ordem, considerando a perspectiva de tratamento de um maior número de dados pessoais e complexidade dos processos de trabalho relacionados:

Diretorias da DGA

- Diretoria de Material e Patrimônio (DMP) - Piloto
- Diretoria de Gestão de Pessoas (DGP)
- Diretoria de Saúde (DS)
- Diretoria de Tecnologia da Informação (DTI)
- Diretoria de Infraestrutura (DIE)
- Diretoria de Engenharia e Arquitetura (DEA)
- Diretoria de Orçamento e Finanças (DOF)
- Gabinete da DGA

Diretorias da DGJ

- Diretoria de Cadastro e Distribuição Processual (DCDP)
- Diretoria de Recursos e Incidentes (DRI)
- Diretoria de Documentação e Informações (DDI)
- Gabinete da DGJ

Diretoria vinculada à Presidência

- Diretoria de Suporte à Jurisdição de 1º Grau (DSJPG)

Os trabalhos de mapeamento nas diretorias foram desenvolvidos durante os meses de **abril e maio de 2021** e foram mapeados nessas unidades **521 processos de trabalho** com o tratamento de dados pessoais.

2.2 Mapeamento nos setores da Cúpula do TJSC

Na sequência das diretorias, o mapeamento avançou para os órgãos e unidades vinculados ao gabinete da Presidência, Vice-Presidências e Corregedoria-Geral da Justiça, alcançando mais **42 setores** e suas áreas internas:

Presidência

- Gabinete, Secretaria e Cartório
- Núcleo Administrativo
- Núcleo Financeiro
- Núcleo Jurídico
- Coordenadoria de Magistrados
- Comissões vinculadas à Presidência
- Assessoria de Cerimonial
- Casa Militar
- Núcleo de Inteligência e Segurança (NIS)
- Assessoria de Planejamento (ASPLAN)
- Assessoria de Precatórios
- Auditoria Interna
- Núcleo de Comunicação Institucional (NCI)
- Ouvidoria
- Grupo de Monitoramento e Fiscalização (GMF)
- Coordenadoria (CEIJ)
- Coordenadoria (CEVID)
- Coordenadoria (COJEPMEC)

1ª Vice-Presidência

- Gabinete e Assessoria
- Comissão de Concurso

2ª Vice-Presidência

- Gabinete e Assessoria
- NUGEP

3ª Vice-Presidência

Corregedoria-Geral da Justiça (CGJ)

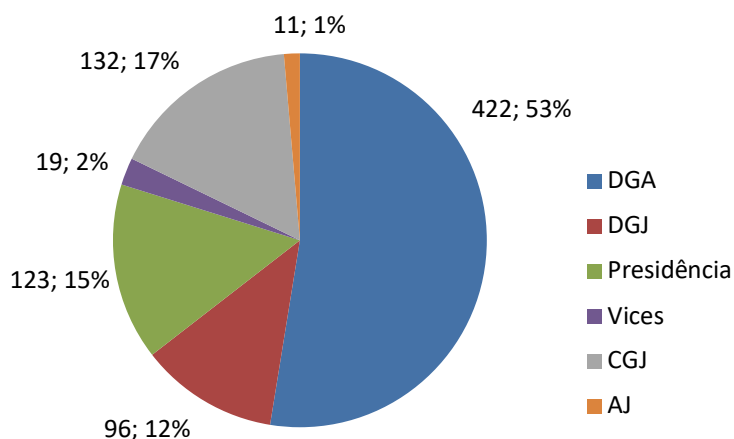
- Gabinete do Corregedor-Geral
- Gabinete do Corregedor-Geral do Extrajudicial
- Secretaria e Assessorias
- Central de Atendimento
- Assessoria de Informática
- Assessoria de Custas
- CEJA
- Divisão Administrativa
- Divisão Judiciária
- Núcleos I, II, III, IV e V

Os trabalhos junto aos órgãos vinculados ao gabinete da Presidência, Vice-Presidências e Corregedoria-Geral da Justiça desenvolveram-se nos meses de **junho e julho de 2021**, sendo que o mapeamento levantou **271 processos de trabalho** com o tratamento de dados pessoais.

Por fim, no mês de agosto, foi realizado o mapeamento na Academia Judicial (AJ), onde foram identificados **11 processos de trabalho** com o tratamento de dados pessoais.

3. RESULTADOS

O 1º mapeamento de processos de trabalho com o tratamento de dados pessoais do TJSC identificou um total de **803 processos**, distribuídos da seguinte forma:



Destes, foram identificados 169 processos de trabalho com dados pessoais que se originam de outras unidades administrativas do TJSC ou que possuem tratamento em mais de um setor.

Todas as unidades administrativas acionadas para a realização do mapeamento apontaram pelo menos um processo de trabalho com o tratamento de dados pessoais. A maior quantidade foi registrada pela Diretoria de Gestão de Pessoas, que mapeou 196 processos de trabalho.

A seguir são apresentados dados estatísticos das respostas fornecidas, com detalhamento das principais constatações efetuadas:

3.1. Questão 5 – Bases Legais

Foram informadas as seguintes bases legais para o tratamento de dados pessoais nos processos de trabalho relacionados:

Bases Legais	Quantidade	Porcentagem
Execução das atribuições legais do TJSC, em atenção a sua finalidade pública	368	46%
Cumprimento de uma lei ou de obrigação estabelecida pelos órgãos reguladores	332	41%
Legítimo interesse do TJSC	25	3%
Execução de obrigações ou procedimentos previstos em contrato em que o titular é parte	21	3%
Exercício regular de direitos em processo judicial, administrativo ou arbitral	20	2%
Execução de política pública, baseada em norma, contrato, convênio ou outro instrumento	12	1%
Cuidados com a saúde, realizados por profissionais de saúde ou autoridade sanitária	12	1%
Consentimento obtido do titular dos dados em documento impresso ou meio eletrônico	8	1%
Proteção da vida ou da incolumidade física do titular ou de terceiro	5	1%

Conforme já esperado, a grande maioria dos processos de trabalho, no caso 87%, possui como base legal para o tratamento de dados pessoais o disposto no artigo 23 da LGPD (referente à execução pelo TJSC de suas atribuições legais, em atenção a sua finalidade pública) e no artigo 7º, II (cumprimento de obrigação legal ou regulatória).

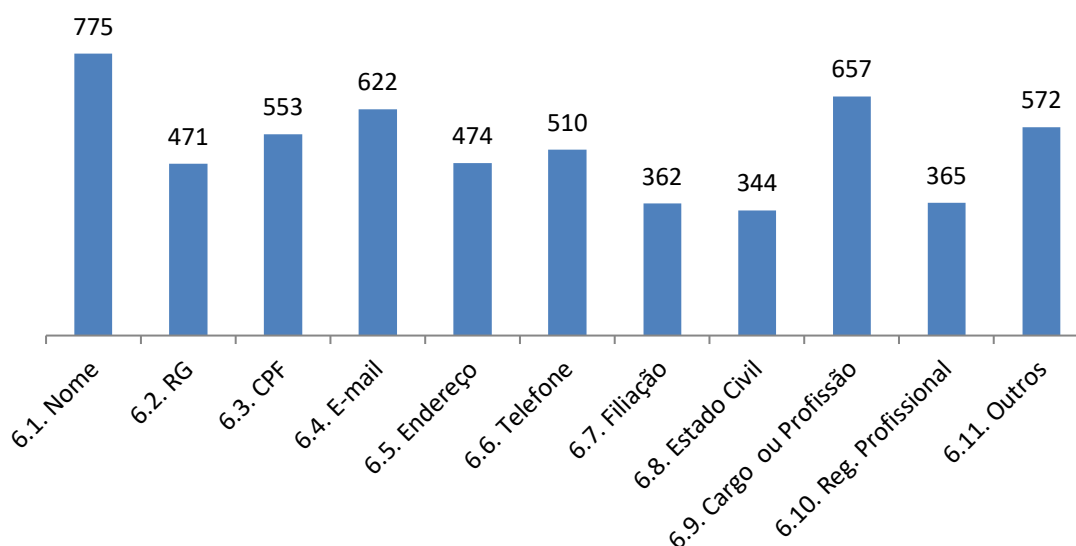
As bases legais relacionadas à realização de estudos por órgãos de pesquisa e à proteção do crédito não foram mencionadas no mapeamento.

Verificou-se, ainda, o registro do legítimo interesse como base legal para 25 processos de trabalho, os quais, numa análise perfunctória, carecem de revisão junto aos setores, a saber: CGJ, 1ª Vice-Presidência, NCI, Asplan, Casa Militar, DGA, DGJ e DTI.

3.2. Questão 6 – Dados Pessoais

Na identificação dos dados pessoais tratados, verificou-se que em 99% dos processos indicados foi confirmado o tratamento de mais de um dado pessoal.

A seguir é apresentada a frequência que os dados pessoais pré-configurados na matriz foram selecionados pelos setores, nos processos de trabalho relacionados.



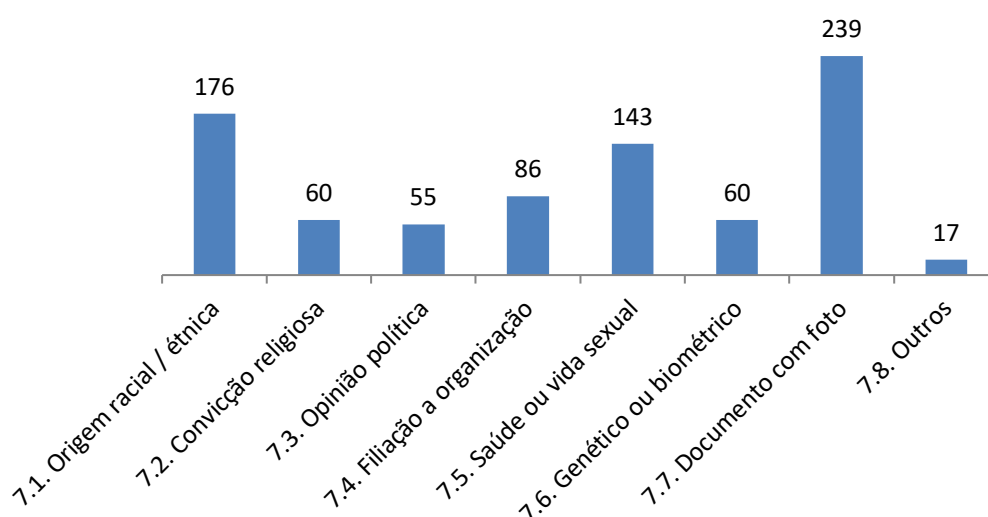
Destacam-se, entre os dados pessoais apontados: nome (97%), cargo ou profissão (82%), e-mail (77%) e CPF (69%). Tais dados, na grande maioria dos processos onde são tratados, estão associados a dados de magistrados, servidores ou advogados.

A questão “6.11 – Outros dados pessoais”, por ser aberta, permitiu a especificação de dados pessoais não listados nos itens anteriores, os quais foram informados em 572 processos de trabalho. Outros dados pessoais indicados pelos respondentes: certidão de nascimento, certidão de óbito, conta bancária, nº do PIS/PASEP, nº do eSocial, Carteira de Trabalho, renda pessoal, passaporte, idade, gênero, naturalidade, nacionalidade, apelido, título de eleitor.

3.3. Questão 7 – Dados Pessoais Sensíveis

Os dados pessoais sensíveis aparecem em quantidade bastante inferior aos dados pessoais comuns. Documento com foto e origem racial e étnica destacam-se, sendo indicados em 30% e 22% dos processos de trabalho, principalmente naqueles relacionados à realização de cadastros, seja para magistrados e servidores ou para o público externo.

Verificou-se que apenas a DMP informou que não efetua o tratamento de dados pessoais sensíveis, em 11 dos 13 processos que relacionou.

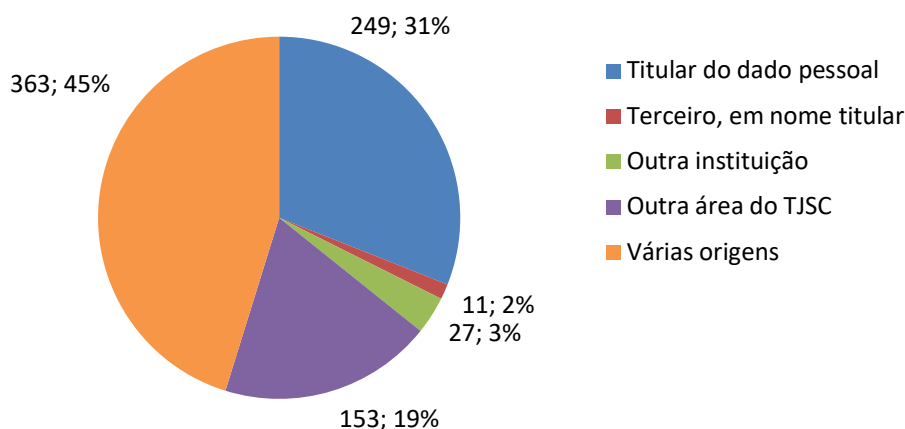


A questão “7.8 – Outros dados pessoais sensíveis”, por ser aberta, permitiu a especificação de dados pessoais sensíveis não listados nos itens anteriores, os quais foram informados em 17 processos de trabalho. Outros dados pessoais indicados pelos respondentes: assinatura, digital, tipo sanguíneo, fotos diversas.

Muitos dos itens informados nessa resposta possuem correspondentes entre os itens pré-configurados ou são apenas dados pessoais comuns e foram ajustados nas planilhas encaminhadas pelos setores.

3.4. Questão 8 – Origem da coleta dos dados

Essa questão indica, basicamente, se o dado pessoal tratado no processo de trabalho é fornecido pelo titular, proveniente de outra área do TJSC ou se é obtido externamente. A distribuição das origens dos dados pessoais é a seguinte:

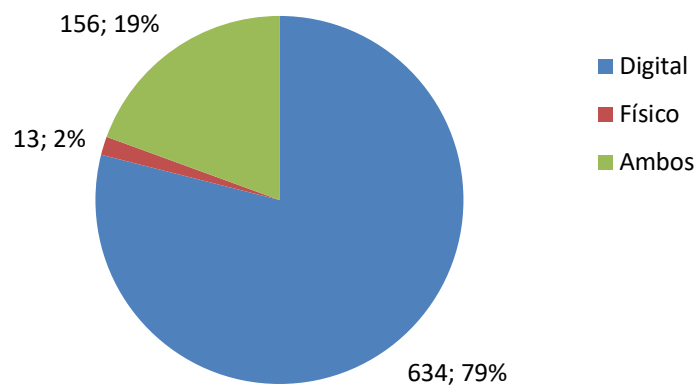


Verificou-se, a partir do cruzamento com outras respostas, que os dados pessoais de todos os 27 processos onde a origem é externa e os 153 que são obtidos de outra área do TJSC são fornecidos ao setor responsável pelo processo de trabalho por um sistema informatizado. O mesmo fato se verifica na grande maioria das respostas que indicam várias origens.

Registra-se, ainda, que o fornecimento de dados pessoais pelo próprio titular ou seu representante legal soma 260 ocorrências e alcança 1/3 dos casos, repercutindo na forma como o TJSC se comunica com o titular de dados pessoais, diante das exigências contidas na LGPD.

3.6. Questão 9 – Tipo dos dados

O dados pessoal em formato digital foi indicado em 98% processos de trabalho relacionados, considerando-se os somente digitais e aqueles que são fornecidos em ambos os formatos (físico e digital):



Essa constatação, reafirma o aspecto já mencionado de que a maioria dos dados pessoais tratados são provenientes de sistemas, acessos a bancos de dados ou formulários eletrônicos.

As unidades administrativas que recebem dados exclusivamente de origem física em seus processos de trabalho são: a DIE, em serviços de postagem e transporte internos de documentos; a DGP, no registro de documentação de aposentados; a DDI, no processamento de processos físicos, protocolização de documentos em processos administrativos e gestão de crachás/identidades funcionais; a DCDP, na recepção e registro de documentação de apenados; e a DRI, na gestão de terceirizados.

3.6. Questão 10 – Nome do sistema ou local onde os dados são armazenados

Considerando que a grande maioria dos dados pessoais tratados são digitais, a identificação do sistema ou local da infraestrutura de TI onde eles são armazenados é fundamental para o conhecimento das questões de segurança da informação relacionadas à proteção desses dados pessoais, bem como a posterior definição de procedimentos e políticas que promovam o seu tratamento adequado.

Assim sendo, procurou-se não estabelecer uma resposta pré-configurada, deixando esta questão aberta para o livre preenchimento pelas unidades administrativas que efetuaram o mapeamento.

Entre os sistemas e ferramentas digitais disponibilizados pelo TJSC, foram relacionados os seguintes:

- Assistência Judiciária
- Banco de Talentos
- Bancos de Dados diversos
- BNMP
- Cadastro de Magistrados
- Central de Atendimento Eletrônico
- Control Desk

- Controle de Acesso
- CUIDA
- DIRF
- DMPAccess
- eConsig
- eProc
- ERP
- e-SFinge
- FCDL
- Folha de pagamento
- Gmail
- Google Drive
- InfoJud
- i-Pen
- iSTJ e iSTF
- Malote Digital
- Mentor
- Notorium
- Outlook Mail
- Pastas de rede
- Pastas locais
- Pergamun
- PJSC Conecta
- Planilhas Excel
- Power BI
- Renajud
- Rol de Antecedentes Criminais
- SAJ
- SCUA
- SEEU
- SEI
- SGDD
- SIAFIJUD
- SIDEJUD
- SIGEF
- SisbaJud
- SisClínica
- SISP
- Sistema de Auxílio Creche
- Sistema de Auxílio Saúde
- Sistema de Certidões
- Sistema de Controle de Terceirizados
- Sistema de Convocação de Concursos
- Sistema de Correição Integrada
- Sistema de Histórico Funcional
- Sistema de Jurisdição Delegada
- Sistema de Precatórios
- Sistema de Promoções
- Sistema de Recursos Humanos
- Sistema de Ressarcimento de Atos
- Sistema do NIS
- SRH
- Suricato
- Workflow

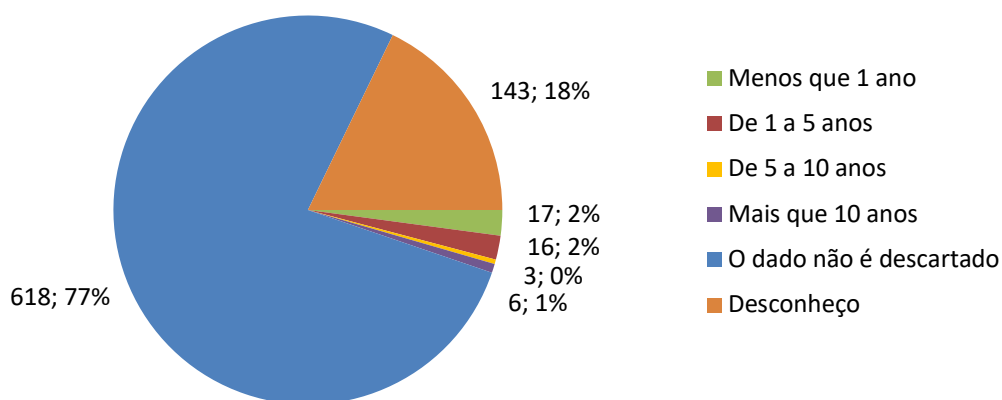
Verificou-se que grande parte dos dados pessoais indicados são armazenados no Sistema Eletrônico de Informações, o qual foi indicado em 446 processos de trabalho, correspondendo a 56% do total de processos mapeados. O segundo maior repositório de dados pessoais apontado foi o sistema de e-mail, com 14% de todos os processos relacionados (115 ocorrências).

Um ponto importante a ser observado é que ambos os sistemas são, notadamente, repositórios de documentos digitais ou digitalizados e de informações desestruturadas, resultando em conjuntos de dados de difícil verificação e controle.

Foram informados, também, arquivos físicos setoriais para o armazenamento de documentos físicos contendo dados pessoais, eventualmente recepcionados pelos setores.

3.7. Questão 11 – Período de tempo de retenção dos dados

A grande maioria das respostas apresentadas (77%) indicou que os dados pessoais tratados no processo de trabalho não são descartados. Os demais períodos de retenção de dados apresentam valores pouco significativos.



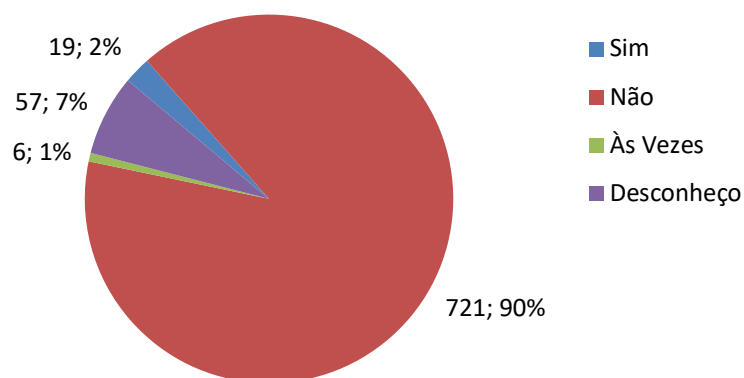
Tal constatação é indício de uma possível desconformidade com os artigos 15 e 16 da LGPD, que disciplinam a eliminação dos dados pessoais com o término do tratamento destes.

Outro ponto a ser observado é a informação em 143 processos de trabalho (18%) a respeito do desconhecimento da retenção dos dados pessoais tratados nos processos, indicando uma fragilidade na governança desses processos de trabalho e sistemas envolvidos.

3.8. Questão 12 – Anonimização ou criptografia dos dados

O presente item procurava identificar a existência de métodos mais elaborados de proteção dos dados pessoais tratados no processo, como a eliminação de qualquer referência, direta ou indireta, dos dados armazenados a um indivíduo (anonimização) ou a substituição das informações existentes por outras cifradas ou irreconhecíveis (criptografia).

A resposta à pergunta “Os dados desse processo são anonimizados ou criptografados” apresentou a seguinte distribuição nos processos mapeados:

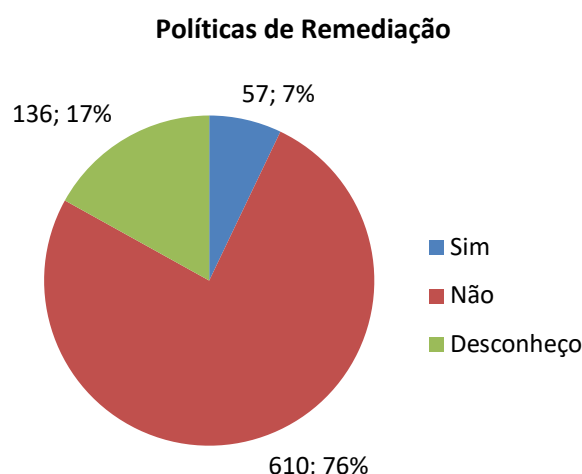
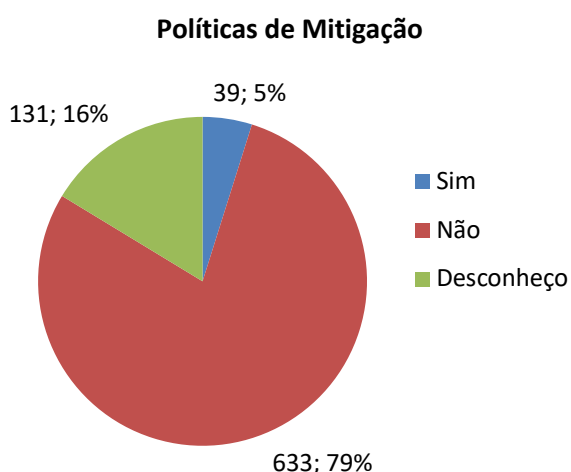


Conforme é possível constatar, 90% dos processos mapeados (721) não possuem a aplicação de qualquer técnica de anonimização ou criptografia para a proteção dos dados pessoais tratados.

Excluídos os 57 processos onde o setor não soube informar, tem-se apenas 25 processos (3%) onde foi apontado o uso de alguma técnica de anonimização ou criptografia. Os setores que indicaram o uso dessas técnicas em seus processos foram: o Gabinete da Presidência, a 1ª e a 2ª Vice-Presidências, o CEIJ, o NIS, a DOF e a DMP. Em que pese o baixo número de processos com a aplicação de técnicas de anonimização e criptografia, registra-se a existência de boas práticas que podem ser compartilhadas com outros setores do TJSC.

3.9. Questões 13 e 14 – Políticas de mitigação e remediação de incidentes de segurança da informação

No tocante às políticas de segurança da informação, especialmente no que se refere à mitigação e remediação de incidentes, tais como acessos indevidos e vazamentos de dados, nos processos mapeados, verificou-se que grande parte não possui ou desconhece a existência de alguma política.



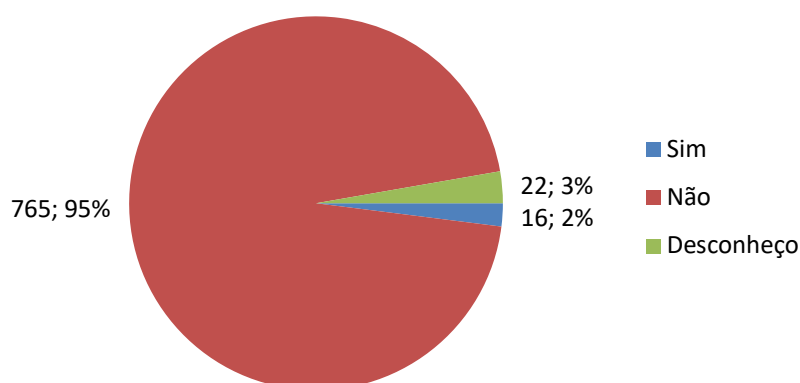
Tanto em relação às políticas de mitigação quanto de remediação de incidentes de segurança da informação, os percentuais de respostas indicando o desconhecimento ou a inexistência de políticas superam 93%, apontando para a necessidade urgente de elaboração, publicação, disseminação e internalização de normas e procedimentos voltados à proteção dos sistemas que suportam os processos de trabalho mapeados.

Os setores que informaram haver políticas de mitigação e remediação em seus processos de trabalho são: Gabinete da Presidência, 2ª Vice-Presidência, NIS, Casa Militar, CGJ, DGA, DGP, DS, DMP, DOF, DTI e DCDP.

Destaque para a DS, que informou 11 processos com políticas de mitigação de incidentes de segurança e para a CGJ e DMP que indicaram processos com políticas de remediação de incidentes em 21 e 12 processos, respectivamente.

3.10. Questão 15 – Tratamento internacional de dados

A indicação de que os dados pessoais do processo são tratados em outro país foi efetuada em apenas 16 processos, representando apenas 2% do total dos processos mapeados.

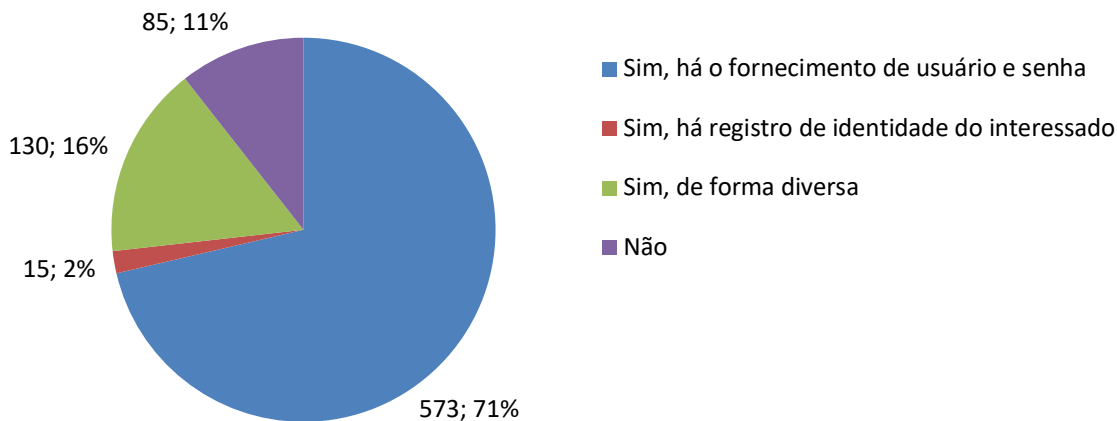


Verificou-se que parte das respostas positivas são decorrentes da utilização de sistemas baseados em plataformas hospedadas em outros países, tais como as ferramentas do Google e da Microsoft. Setores como o Gabinete da Presidência, Asplan, CEIJ, DMP e CGJ mencionaram a utilização de tais ferramentas.

Os processos de trabalho que efetivamente compartilham dados com outros países, para atingimento da finalidade descrita são: os relacionados à adoção internacional mapeados pela CEJA da CGJ; a emissão de alvarás pela Assessoria de Precatórios; o processamento de serviços postais internacionais pela DIE; a gestão de cadastros financeiros de servidores e magistrados realizada pela DGP; e a realização de licitações internacionais pela DMP.

3.11. Questão 16 – Controle de acesso aos dados

A necessidade de utilização de um usuário pré-cadastrado e uma senha para acesso a dados pessoais foi indicada em 573 processos mapeados (71%). O resultado é compatível com o principal tipo de dados identificado (digital) e a característica de grande parte dos sistemas utilizados no TJSC, que disponibilizam serviços para servidores e magistrados previamente cadastrados na base de dados de usuários internos.

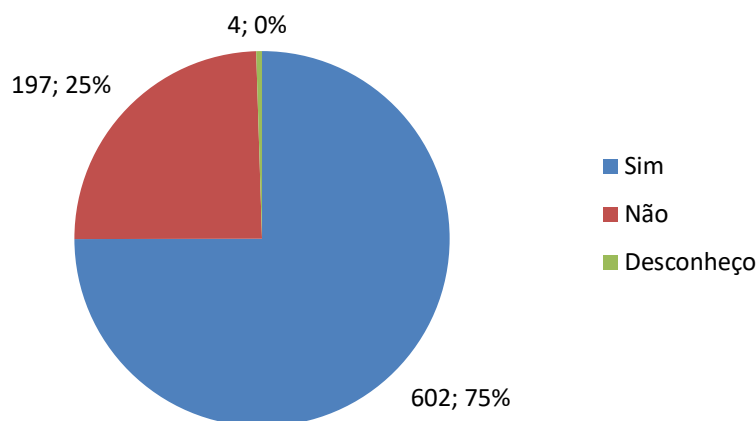


A existência de controle de acesso por senha, com a identificação dos perfis dos usuários que acessam os sistemas, é uma boa prática no sentido da proteção de dados pessoais tratados nos processos suportados por esses sistemas.

Registra-se, ainda, que foi indicado o registro da identidade do interessado em 15 processos mapeados pela Auditoria Interna, DGP e DTI, especialmente para fins de emissão de certidões e certificados digitais, responsabilização por serviços prestados, processos de aposentadoria e registro de dependentes.

3.12. Questão 17 – Acesso aos dados por outras áreas do TJSC

As unidades administrativas indicaram que $\frac{3}{4}$ dos processos mapeados possui dados pessoais acessados por outras unidades do TJSC:



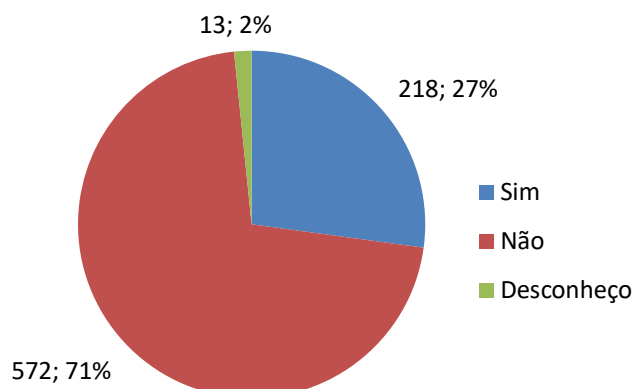
Mesmo que o número de processos que tramitam por vários setores seja menor, novamente confirma-se o cenário de uma utilização generalizada de sistemas, com o armazenamento de dados pessoais em bancos de dados internos, aos quais é franqueado o acesso aos usuários de outros setores do TJSC, de modo a facilitar a obtenção de informações para propósitos específicos do setor.

Verificou-se, nos processos que indicaram não existir acesso aos dados pessoais por outras áreas do TJSC, que uma análise mais aprofundada dos sistemas utilizados e das funcionalidades disponibilizadas por estes pode indicar que há, sim, o acesso de usuários externos ao setor, aumentando o índice supracitado.

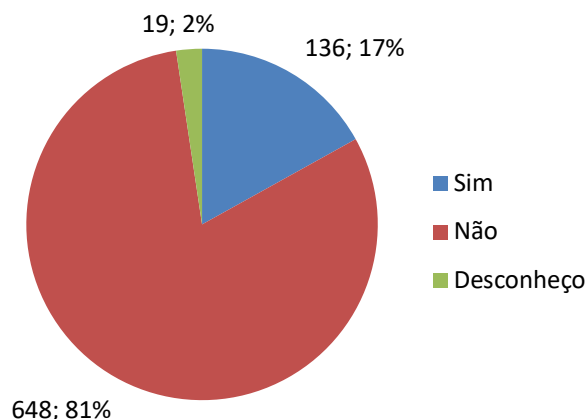
3.13. Questões 18 e 19 – Compartilhamento de dados

As respostas a essas questões indicam se há o compartilhamento de dados pessoais dos processos mapeados para instituições externas, governamentais e não governamentais. Da análise realizada pelas unidades administrativas, obteve-se o seguinte resultado:

Compartilhamento Externo Governo



Compartilhamento Outras Instituições

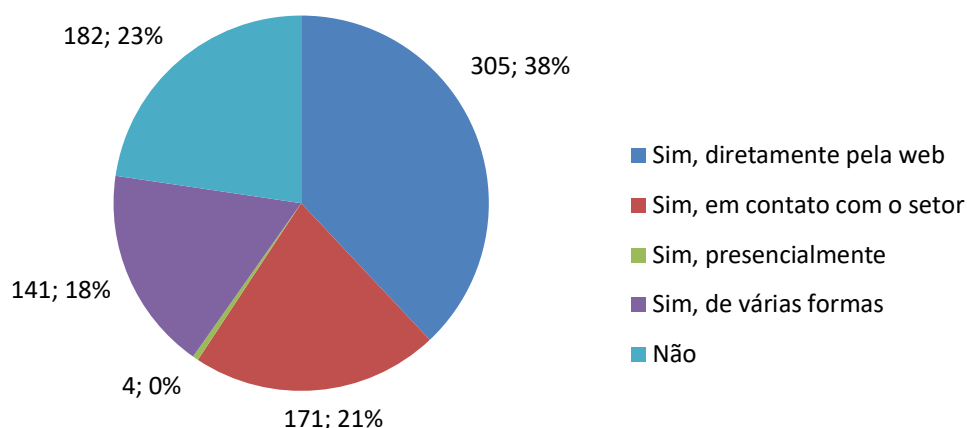


O compartilhamento de dados com instituições governamentais aparece em 218 processos mapeados (27%) e está concentrado no envio de informações para prestação de contas ao Conselho Nacional de Justiça, a partir de disposições normativas do órgão regulador, e ao Tribunal de Contas do Estado de SC; informações processuais aos órgãos do Judiciário Federal; e informações de magistrados e servidores aos órgãos de previdência do Estado de SC.

Verificou-se, em metade das respostas indicando haver o compartilhamento de dados, que não houve a especificação dos órgãos para os quais os dados são enviados, dificultando uma análise mais aprofundada das respostas apresentadas.

3.14. Questão 19 – Consulta dos dados pessoais pelo titular

Da análise das informações apresentadas nessa questão, extrai-se que em grande parte dos processos de trabalho (77%), é permitido ao titular ter acesso aos seus dados pessoais:



Isso demonstra a preocupação do TJSC em dar transparência aos cidadãos sobre os dados que armazena e estar em conformidade com os princípios da LGPD. Da mesma forma, ao oferecer acesso direto aos dados pessoais pela web em 305 processos de trabalho (38%), verifica-se o

investimento do TJSC em oferecer serviços para que o cidadão possua autonomia e exerça a autodeterminação informativa.

Por outro lado, é importante destacar que tais serviços estejam acompanhados das melhores técnicas de segurança da informação e para impedir o acesso indevido a dados pessoais.

4. CONCLUSÃO

O trabalho de mapeamento realizado por todo o TJSC traz uma fotografia do tratamento de dados pessoais nos processos vigentes. Tais informações são importantes para o atendimento de solicitações de confirmação de tratamento de dados pessoais por titulares, para a elaboração de relatórios de impacto e, em última instância, contribui para a adequação do TJSC à LGPD.

Contudo, considerando que se trata de um registro estático, sugere-se que o presente mapeamento de processos seja revisto a cada 2 anos, permitindo o ajuste dos processos à nova realidade, a inserção de novos processos de trabalho ou a exclusão daqueles que deixaram de existir.

A constatação de que o SEI é o principal repositório de dados pessoais, traz o indicativo de que os dados pessoais contidos no referido sistema tramitam entre vários setores do TJSC, visto que esse sistema é utilizado internamente para o trâmite de todos os processos administrativos, com origem interna e também a partir da protocolização de pedidos externos. Ajustes no SEI para sua adequação LGPD, certamente trará inúmeros benefícios para a segurança dos processos de trabalho e o incremento da integridade e inviolabilidade dos dados pessoais armazenados nesse sistema.

O mapeamento mostrou a carência do TJSC no tocante a políticas de segurança da informação, notadamente políticas de retenção e descarte de dados, bem como de diretrizes para aplicação de técnicas de anonimização ou criptografia de dados, para a proteção especialmente de dados pessoais sensíveis.

Recomenda-se, de imediato, a definição de perfis de usuários e autorizações para acesso a sistemas, permitindo uma melhor gestão dos sistemas e serviços que podem ser disponibilizados a magistrados e servidores, bem como o controle e auditoria dos acessos realizados.

Em que pese não terem sido verificadas políticas, diretrizes e procedimentos relacionados à segurança da informação efetivamente implantadas, a existência de boas práticas é um bom sinal. Sugere-se, nesse sentido, que tais práticas sejam disseminadas junto aos setores que possam absorvê-las pela similaridade dos processos de trabalho vigentes.

Outrossim, reforça-se a necessidade de se manter um programa de capacitação constante, para que os temas e as orientações relacionados à privacidade e à proteção de dados pessoais sejam internalizados por magistrados e servidores que atuam nas unidades administrativas.