Tribunal Regional do Trabalho da 15ª Região

IARA CRISTINA GOMES

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE - 2022

JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 15ª Região (Campinas)

ASSESSORIA DE GESTÃO ESTRATÉGICA

Sumário

1 Apresentação

O uso de dados pessoais tem se tornado cada dia mais frequente, como decorrência lógica da globalização da economia e do avanço tecnológico. Nesse contexto, um cenário desafiador se apresenta: incentivar a utilização de ferramentas virtuais - as quais podem contribuir sobremaneira para a otimização de tempo e para o melhor uso de recursos -, sem, contudo, descuidar das formalidades legais e dos direitos assegurados aos titulares de dados.

Diante desse cenário, entrou em vigor, em maio de 2018, na União Europeia, o Regulamento Geral sobre Proteção de Dados (também conhecido como GDPR), norma que inspirou a edição de outras análogas em todo o mundo, tal como ocorreu no Brasil, com a edição da Lei n.º 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

A publicação da Lei Geral de Proteção de Dados (LGPD) representa um importante avanço na consolidação dos direitos do cidadão e grande desafio para as instituições se adequarem aos dispositivos estabelecidos por esse normativo. A Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O setor público é um dos principais agentes de tratamento de dados pessoais e a LGPD criou um alerta às organizações sobre a proteção de dados de seus usuários, o que vem acarretar esforços cada vez maiores para manter o controle e a segurança dos sistemas de armazenamento, *sites* e outros setores vinculados à captura de informações de seus titulares.

O vazamento de informações é algo que infringe a lei. Portanto, é urgente a compreensão de que a cautela não cabe somente às partes do processo, mas, aos julgadores, servidores, estagiários, colaboradores, auxiliares da justiça, cujos dados pessoais são tratados no sistema judicial.

Assim, sendo as normas gerais contidas na LGPD de interesse nacional, as quais devem ser observadas pela União, Estados, Distrito Federal e Municípios, urge que os entes federativos e seus respectivos órgãos adotem providências para adequar-se à Lei Nº 13.709/2018.

Nesse sentido, surge o presente **Programa de Governança em Privacidade** do Tribunal Regional do Trabalho da 15ª Região, o qual se propõe a ser o instrumento orientador de conformidade da Corte à Lei Geral de Proteção de Dados Pessoais.

2 Introdução

O **Programa de Governança em Privacidade** do Tribunal Regional do Trabalho da 15ª Região é o documento que norteia a implementação da Lei n.º 13.709 (LGPD), de 14 de agosto de 2018, no âmbito do Regional.

Neste sentido, já foram iniciadas ações voltadas para a proteção de dados pessoais com as publicações da Portaria GP Nº 025/2021, de 8 de abril de 2021, instituindo o Comitê Gestor de Proteção de Dados Pessoais (CGPD) e o Grupo de Trabalho Técnico, e do Ato Regulamentar GP Nº 006/2021, de 3 de agosto de 2021, que instituiu a Política de Privacidade e Proteção de Dados Pessoais - PPPDP.

A referida Lei estabelece regras específicas para o tratamento, o uso e a proteção da privacidade dos dados pessoais coletados e gerados por aplicações e serviços digitais, bem como, em meios físicos. A LGPD empodera os titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos durante toda a existência do tratamento das informações pela Instituição. A Lei prevê um conjunto de ferramentas, que, no âmbito público, traduzem-se em mecanismos que aprofundam obrigações de transparência ativa e passiva.

Ao estruturar o planejamento da implementação da Lei Geral de Proteção de Dados no TRT-15, o **Programa de Governança em Privacidade** tem por parâmetro, além da própria LGPD, normas correlatas no plano nacional e internacional, guardando consonância com o arcabouço jurídico pátrio atinente à proteção de dados pessoais e com os compromissos assumidos pelo Brasil relativos ao tema, a exemplo da Parceria para Governo Aberto (*Open Government Partnership – OGP*) - iniciativa internacional que pretende difundir e incentivar globalmente práticas governamentais relacionadas à transparência dos governos, ao acesso à informação pública e à participação social.

O **Programa de Governança em Privacidade** reúne diretrizes para que o Tribunal, por meio de um esforço conjunto e sinérgico, adote as medidas necessárias para assegurar a observância dos princípios estatuídos na LGPD referentes aos direitos dos titulares de dados pessoais.

Um dos referenciais teóricos utilizados para a elaboração do referido Programa foi o Guia de Boas Práticas da LGPD, o qual visa fornecer orientações aos órgãos e entidades da administração pública federal, autárquica e fundacional, para as operações de tratamento de dados

pessoais, conforme previsto no art. 50 da Lei nº 13.709/18, além de detalhar métodos e formas de diferenciação das mais diversas situações com as quais irão se deparar os servidores públicos responsáveis por operar ou controlar a aplicação da aludida lei.

Ainda como referenciais teóricos adotados para constituir o Programa de Governança em Privacidade, citem-se os Guias Operacionais para conformidade às diretrizes trazidas pela LGPD.

Na construção do **Programa de Governança em Privacidade** foram considerados, à luz dos dispositivos pertinentes da LGPD, aspectos atinentes ao Contexto Organizacional, à Liderança, à Capacitação, à Conformidade do Tratamento, aos Direitos do Titular, ao Compartilhamento de Dados Pessoais, à Violação de Dados Pessoais e às Medidas de Proteção, por meio uma abordagem atinente a aspectos de Governança, de Conformidade Legal e Respeito aos Princípios de Transparência e Direitos do Titular, de Rastreabilidade, de Adequação de Contratos e Relações com Parceiros, de Segurança da Informação, e de Violação de Dados.

É válido destacar que o **Programa de Governança em Privacidade** para conformidade do TRT-15 à LGPD será atualizado sempre que necessário, para ajustar-se às determinações da Autoridade Nacional de Proteção de Dados (ANPD) e aos órgãos de controle interno e externo, bem como para melhor esclarecer algum trecho específico, ou diante de eventuais atualizações legislativas ou, ainda, de novos entendimentos preponderantes sobre a matéria.

3 Legislação relacionada

Na elaboração do presente Programa, considerou-se o seguinte arcabouço de normas, as quais contêm previsões autorizando o tratamento de dados:

- **Lei n° 9.507/1997**, que regula o direito de acesso a informações e disciplina o rito processual do *habeas* data.

- **Lei n° 9.784/1999**, que regula o processo administrativo no âmbito da Administração Pública Federal.

- **Lei n° 12.527/2011** (Lei de Acesso à Informação), que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

- **Decreto n° 7.724/2012**, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

- **Lei n° 12.965/2014** (Marco Civil da *Internet*), que estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil.

- **Decreto n° 8.771/2016**, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da *Internet*), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

- **Lei n° 13.444/2017**, que dispõe sobre a Identificação Civil Nacional (ICN).

- **Lei n° 13.460/2017,** que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

- **Decreto n° 9.278/2018,** que regulamenta a Lei nº 7.116, de 29 de agosto de 1983, que assegura validade nacional às Carteiras de Identidade e regula sua expedição.

- **Lei n° 13.709/2018,** Lei Geral de Proteção dos Dados – LGPD.

- **Decreto n° 9.723/2019**, que altera o Decreto nº 9.094, de 17 de julho de 2017, o Decreto nº 8.936, de 19 de dezembro de 2016, e o Decreto nº 9.492, de 5 setembro de 2018, para instituir o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo da apresentação de outros documentos do cidadão no exercício de obrigações e direitos ou na obtenção de benefícios e regulamentar dispositivos da Lei nº 13.460, de 26 de junho de 2017.

- **Lei n° 13.853/2019**, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

- **Decreto n° 10.046/2019**, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

4 Objetivos

Com a implementação deste Programa, pretende-se alcançar o seguinte objetivo geral:

Estabelecer regras de segurança, de boas práticas e de governança, e procedimentos envolvendo a proteção de dados pessoais no âmbito do Tribunal Regional do Trabalho da 15ª Região e estar em conformidade com a LGPD.

Ademais, pretende-se alcançar os seguintes objetivos específicos:

Conferir transparência sobre o uso dos dados pessoais pelo TRT-15 e fomentar a cultura de Proteção de Dados Pessoais no âmbito do Tribunal.

Oferecer maior clareza à gestão sobre os ciclos de vida dos dados pessoais.

Definir e divulgar as regras de proteção e tratamento de dados pessoais pelo Tribunal.

Prover diretrizes para a atuação do Comitê Gestor de Proteção de Dados Pessoais (CGPD).

Identificar as atividades prioritárias a serem desenvolvidas para o atendimento das disposições da LGPD.

5 Tratamento de Dados Pessoais

CONCEITOS

Nos termos do art. 5º da LGPD, considera-se:

- **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável (LGPD, art. 5º, I).
- **dado pessoal sensível:** 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 (LGPD, art. 5º, II).
- **dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (LGPD, art. 5º, III).
- **banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (LGPD, art. 5º, IV).
- **titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (LGPD, art. 5º, V).
- **controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI).
- **operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, art. 5º, VII).
- **encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD (LGPD, art. 5º, VIII).
- **agentes de tratamento**: o controlador e o operador (LGPD, art. 5º, IX).

- **tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (LGPD, art. 5º, X).
- **anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (LGPD, art. 5º, XI).
- **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (LGPD, art. 5º, XII).
- **bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (LGPD, art. 5º, XIII).
- **eliminação**: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado (LGPD, art. 5º, XIV).
- **transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (LGPD, art. 5º, XV).
- **uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (LGPD, art. 5º, XVI).
- **relatório de impacto à proteção de dados pessoais (RIPD)**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (LGPD, art. 5º, XVII).
- **órgão de pesquisa**: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (LGPD, art. 5º, XVIII).

- **autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (LGPD, art. 5º, XIX).

PRINCÍPIOS

Nesse aspecto, é imperioso destacar os princípios elencados no art. 6º da LGPD, os quais devem orientar o tratamento de dados pessoais:

> *Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*
> *II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;*
> *III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;*
> *IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;*
> *V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*
> *VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*
> *VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;*
> *VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*
> *IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;*
> *X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*

HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

Nesse sentido, destacam-se as hipóteses de tratamento de dados pessoais trazidas pelo art. 7º da LGPD:

> *Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
> *I - mediante o fornecimento de consentimento pelo titular;*
> *II - para o cumprimento de obrigação legal ou regulatória pelo controlador;*
> *III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;*
> *IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;*
> *V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;*
> *VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*
> *VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;*
> *VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)*
> *IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou*
> *X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.*

No mesmo sentido, importante trazer as hipóteses de tratamentos de dados pessoais sensíveis referidas no art. 11 da LGPD:

> *Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:*
> *I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;*
> *II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:*
> *a) cumprimento de obrigação legal ou regulatória pelo controlador;*
> *b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;*
> *c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;*
> *d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*
> *e) proteção da vida ou da incolumidade física do titular ou de terceiro;*
> *f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)*
> *g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.*

DIREITOS DO TITULAR

A Lei Geral de Proteção de Dados Pessoais empodera os titulares de dados, fornecendo-lhes direitos a serem exercidos perante os controladores de dados, como se pode verificar na tabela abaixo:

Direitos dos titulares de dados que decorrem dos princípios	Princípio correspondente	Referência legislativa (LGPD)
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.	Princípio da finalidade	Art. 6º, I
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da adequação	Art. 6º, II
Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.	Princípio da necessidade	Art. 6º, III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.	Princípio do livre acesso	Art. 6º, IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.	Princípio da qualidade dos dados	Art. 6º, V
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.	Princípio da transparência	Art. 6º, VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas 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 difusão.	Princípio da segurança	Art. 6º, VII

Direitos dos titulares de dados que decorrem dos princípios	Princípio correspondente	Referência legislativa (LGPD)
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	Princípio da prevenção	Art. 6º, VIII
Direito de não ser discriminado de forma ilícita ou abusiva.	Princípio da não discriminação	Art. 6º, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.	Princípio da responsabilização e prestação de contas	Art. 6º, X

Nessa esteira, a LGPD não somente assegura aos titulares de dados os direitos decorrentes dos princípios (art. 6º), mas também outros direitos específicos, conforme relacionados na tabela a seguir:

Direitos específicos dos titulares de dados	Referência legislativa (LGPD)
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais.	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento.	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento.	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais.	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.	Art. 9º, § 1º
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado.	Art. 8º, § 5º
Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento.	Arts. 8º, § 6º e 9º, § 2º

Direitos específicos dos titulares de dados	Referência legislativa (LGPD)
Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras): finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular, com menção explícita aos direitos contidos no art. 18.	Art. 9º
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento.	Art. 8º, § 6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou, ainda, para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos.	Art. 9º, § 3º
Direito de ser informado sobre a utilização dos dados pela administração pública para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa.	Art. 7º, III e IV c/c art. 7º, § 1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização.	Art. 7º, § 3º
Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento. No caso da Administração Pública Federal (APF), em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento.	Art. 7º, § 5º
Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador.	Art. 10, § 1º
Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador.	Art. 10, § 2º
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa.	Art. 11, II, c
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para: tratamento de dados sensíveis no cumprimento de obrigação legal ou regulatória pelo controlador; ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.	Art. 11, § 2º
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular).	Art. 11, § 4º

Direitos específicos dos titulares de dados	Referência legislativa (LGPD)
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.	Art. 13
Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública.	Art. 13, § 1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa.	Art. 13, § 2º
Direito ao término do tratamento, quando verificado que: (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento; (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da Lei e resguardado o interesse público; ou (iv) por determinação da autoridade nacional, quando houver violação ao disposto na Lei.	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais.	Art. 16

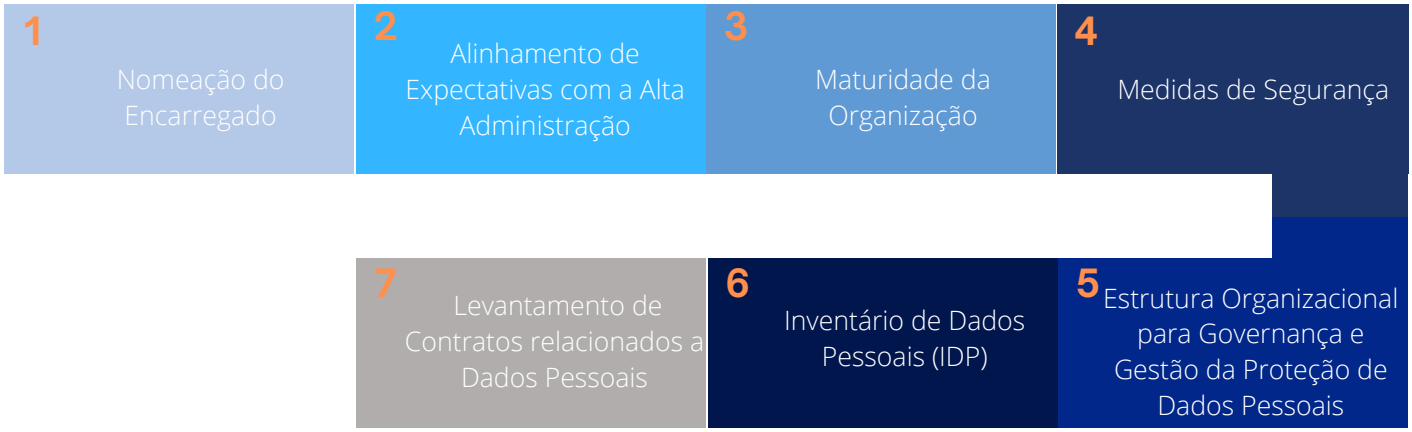
6 Etapas da implementação do Programa de Governança em Privacidade à LGPD

Na Administração Pública, o gerenciamento da privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que os órgãos e entidades precisam prover para conquistar a confiança dos servidores e dos cidadãos e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade.

Para a estrutura do **Programa de Governança em Privacidade** foi utilizada a metodologia do ciclo PDCA (*Plan, Do, Check e Act*), organizada nas seguintes etapas, detalhadas e descritas a seguir:

INICIAÇÃO E PLANEJAMENTO

Nesta etapa, busca-se compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Posteriormente, seguem os principais marcos para ilustrar esta etapa na figura abaixo:



NOMEAÇÃO DO ENCARREGADO

A indicação do encarregado deve acontecer no início da implantação do **Programa de Governança em Privacidade**. Conforme o art. 5º inciso VIII da LGPD, o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. As atividades do encarregado :

- **Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;**
- **Receber comunicações da Autoridade Nacional e adotar providências;**
- **Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção dos dados pessoais; e**
- **Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.**

A Excelentíssima Juíza Auxiliar da Presidência, Lúcia Zimmermann, foi nomeada como Encarregada/DPO, além de compor o Comitê Gestor de Proteção de Dados Pessoais e o Grupo de Trabalho Técnico, conforme Portaria GP 25/2021 publicada em 8 de abril de 2021 pelo Tribunal Regional do Trabalho da 15ª Região.

ALINHAMENTO DE EXPECTATIVAS COM A ALTA ADMINISTRAÇÃO

Ao longo da etapa de Iniciação e Planejamento é importante alinhar as expectativas com a alta administração, priorizando as ações mais urgentes, sem esquecer de mencionar os projetos e as estruturas da organização envolvidas.

Neste sentido, vislumbra-se como essencial a implementação de um programa de conscientização que promova a cultura de proteção de dados em todo o Regional e estabeleça tal postura perante os demais parceiros do TRT-15 e partes interessadas.

MATURIDADE DA ORGANIZAÇÃO

Outro ponto a se analisar é a maturidade da organização, observando fatores como a rastreabilidade de dados - estruturando-os e descrevendo as informações tratadas em cada sistema -, a comunicação com o cidadão e a transparência, elaborando, por exemplo, a política de privacidade e os termos de uso de serviços, bem como a comunicação sobre o uso de *cookies*.

Além de retratar o nível de adequação à LGPD, o índice de maturidade é também utilizado como um indicador de performance e será apresentado na etapa de Monitoramento.

MEDIDAS DE SEGURANÇA

Na etapa de Iniciação e Planejamento, medidas de segurança também devem ser analisadas e adotadas, revisando e propondo aprimoramento das diretrizes e cultura internas. Uma das ferramentas que pode auxiliar na construção do **Programa de Governança em Privacidade** como um todo é o Guia de Boas Práticas da LGPD, o qual propõe caminhos para a sustentabilidade das ações de proteção aos dados pessoais.

ESTRUTURA ORGANIZACIONAL PARA GOVERNANÇA E GESTÃO DA PROTEÇÃO DE DADOS PESSOAIS

Recomenda-se ainda, como suporte para a estrutura do **Programa de Governança em Privacidade**, assim como para a realização das atividades da encarregada provenientes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, o estabelecimento de uma estrutura organizacional para governança e gestão da proteção de dados pessoais, de acordo com o porte da Instituição.

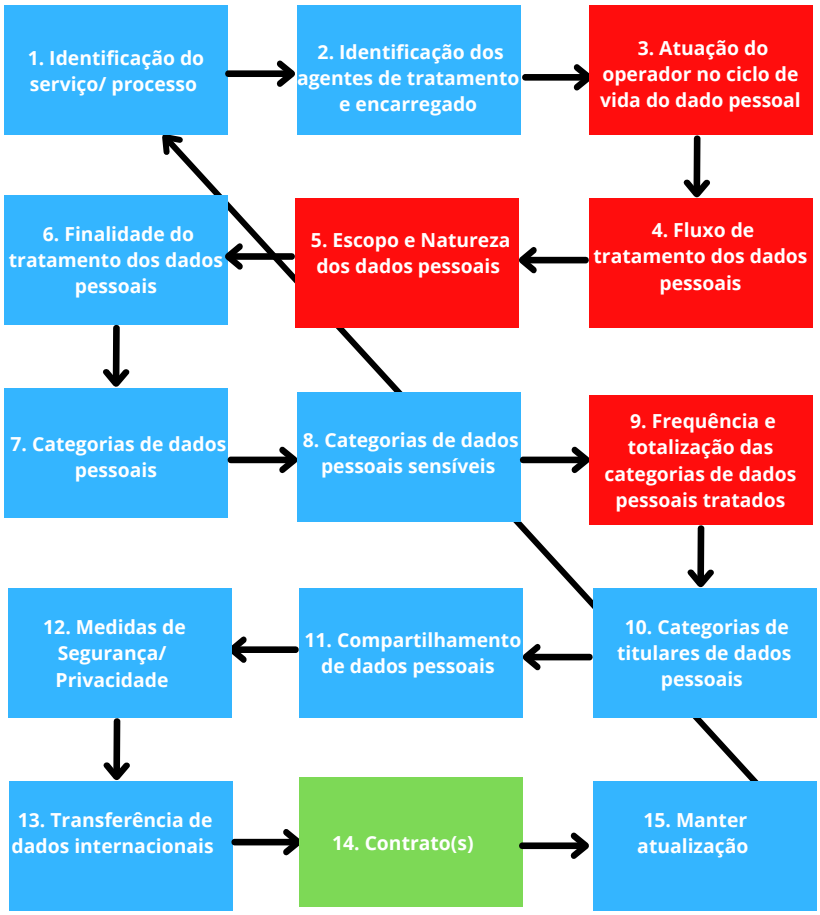
A Presidência do Tribunal Regional do Trabalho da 15ª Região, atenta à importância e ao impacto da LGPD nos diversos processos de trabalho do Regional, publicou a Portaria GP 25/2021 que instituiu o Comitê Gestor de Proteção de Dados Pessoais, que será responsável pela implementação da LGPD no âmbito da Corte e, o Grupo de Trabalho Técnico, de caráter multidisciplinar, que auxiliará a Encarregada do Comitê principal.

INVENTÁRIO DE DADOS PESSOAIS (IDP)

Para a obtenção de um mapeamento dos dados pessoais utilizados pelo TRT-15, é importante a realização de um inventário de dados, especialmente dos dados pessoais, que atenda o artigo 37, da Lei 13.709/2018.

O inventário consiste em uma excelente forma de fazer um balanço do que o Tribunal faz com as informações pessoais, identificando quais dados são tratados, onde estão e que operações são realizadas com eles.

Como sugestão para elaboração do inventário de dados pessoais, a figura a seguir destaca as fases de elaboração do IDP a ser utilizada por cada área do Tribunal:



As fases destacadas em **azul** representam os elementos mínimos para o IDP; as que se encontram em **vermelho** referem-se ao levantamento complementar no inventário de informações que auxiliarão a elaboração do Relatório de Impacto de Proteção de Dados Pessoais - RIPD; e a indicada em **verde** corresponde à identificação das contratações a serem avaliadas na análise preliminar de adequação. Importante ressaltar que todas as informações do IDP subsidiarão o RIPD.

LEVANTAMENTO DE CONTRATOS RELACIONADOS A DADOS PESSOAIS

O levantamento dos serviços que tratam dados pessoais no inventário viabiliza a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais contribui para possíveis e necessárias adequações, tanto nos contratos existentes, quanto nos futuros.

CONSTRUÇÃO E EXECUÇÃO

A partir do texto da LGPD, pode-se inferir que o **Programa de Governança em Privacidade** deve ser projetado para proteger os direitos do cidadão em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes. Assim, na etapa de construção deste Programa, foi considerado os pontos de atenção listados a seguir:

GERENCIAMENTO DE DIREITOS INDIVIDUAIS

O gerenciamento de direitos individuais de privacidade de dados é essencial para a LGPD, como o direito de acessar os dados que um órgão ou entidade mantém sobre os indivíduos, bem como o direito de os atualizar. Os órgãos e entidades devem estar preparados para receber, realizar a triagem e responder consultas e reclamações, podendo sofrer penalidades por não responder de maneira oportuna.

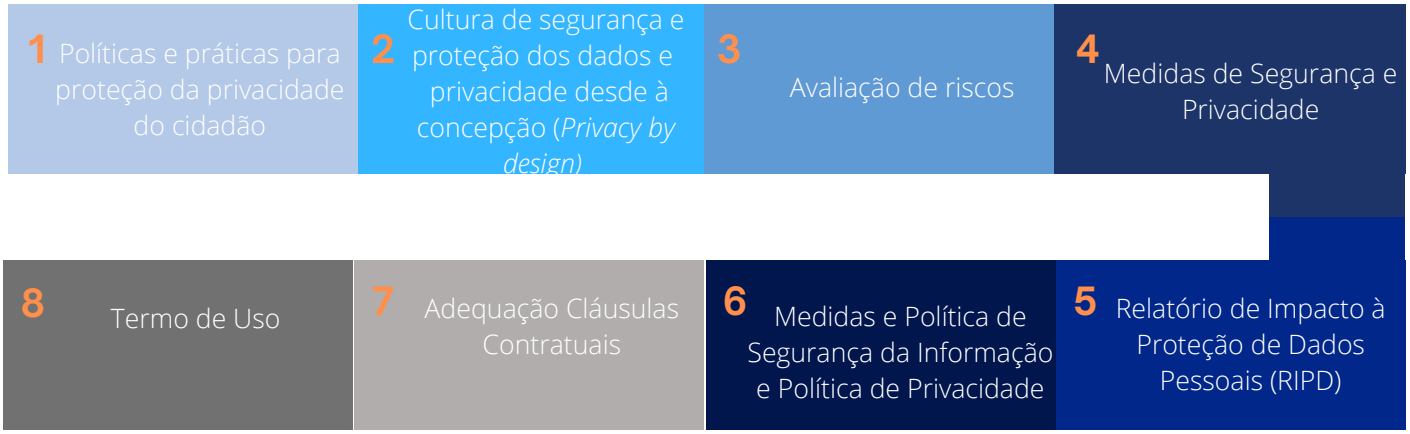
CONSENTIMENTO E RASTREAMENTO DE PREFERÊNCIA

Os cidadãos querem saber se as suas preferências estão sendo honradas. Para o órgão estar posicionado para capturar consentimento e rastrear solicitações de preferências tanto dos titulares dos dados como dos agentes de tratamento ajuda a reduzir a probabilidade de problemas e aumenta a confiança do cidadão.

REDUÇÃO DE RESPONSABILIDADE POR VIOLAÇÃO

A redução da exposição pode ser feita por meio de medidas como, por exemplo, criptografia e anonimização de dados. Os dados devem ser mantidos apenas para sua finalidade.

Nesta etapa, os marcos a serem alcançados seguem discriminados na figura a seguir:



POLÍTICAS E PRÁTICAS PARA A PROTEÇÃO DE DADOS E PRIVACIDADE DO CIDADÃO

As políticas e as práticas de proteção da privacidade do cidadão devem garantir que todo tratamento de dados pessoais seja conhecido e adequado de acordo com a lei. Além disso, é imprescindível a proteção contra mau uso das informações ou, ainda, a revelação inadvertida ou deliberada. Papéis específicos dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais precisam ser revistos, com a ampliação da capacitação dos colaboradores em relação aos novos normativos relativos ao tema "proteção de privacidade".

Informações como a finalidade do órgão e a base legal para tratamento de dados, obtidas no inventário dos dados pessoais, são úteis na construção das operações de tratamento. Tais esclarecimentos auxiliam na determinação dos detalhes do ciclo de vida dos dados pessoais, por exemplo a razão do tratamento, como, onde e por quanto tempo é o armazenamento, entre outros.

Por meio do Ato Regulamentar GP Nº 006/2021, foi instituída a Política de Privacidade e Proteção de Dados Pessoais - PPPDP no âmbito do Tribunal Regional do Trabalho da 15ª Região, a qual pode ser acessada na página do referido Órgão.

CULTURA DE SEGURANÇA E PROTEÇÃO DE DADOS E PRIVACIDADE DESDE A CONCEPÇÃO (PRIVACY BY DESIGN)

A promoção de uma cultura de segurança e proteção de dados é tratada na etapa de construção e de execução do **Programa de Governança em Privacidade** com o intuito de comunicar os **objetivos**, **metas** e **indicadores** utilizados, além de divulgar o papel da Administração Pública como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos.

Capacitação e treinamento devem ser oferecidos para que uma cultura de Privacidade desde a **concepção** (P*rivacy by Design*) seja instituída.

A proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas:

> *Art. 46. Os agentes de tratamento devem 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.*
>
> *§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.*
>
> *§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.*

O conceito de Privacidade desde a **concepção** significa que a proteção de dados deve ser considerada desde o início e seguir durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Essa obrigação de implementação dita que o Tribunal deve limitar a quantidade de dados pessoais coletados, extensão do tratamento, período de armazenamento e acessibilidade ao mínimo necessário para a concretização da sua finalidade.

A medida deve garantir, por exemplo, que nem todos os usuários tenham acesso ilimitado e por tempo indeterminado aos dados pessoais tratados pelo TRT-15.

A privacidade por padrão é obtida por meio da adoção das seguintes práticas:

- **Especificação da finalidade** - os objetivos para os quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao titular dos dados antes ou no momento em que as informações são coletadas. As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se pretende ao tratar os dados pessoais.

- **Limitação da coleta** - a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.

- **Minimização dos dados** - a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve minimizada. A concepção de programas, tecnologias e sistemas de informação e comunicação deve começar com interações e transações não identificáveis, como padrão.

- **Limitação de uso, retenção e divulgação** - o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança.

Quando a necessidade ou uso de dados pessoais não forem claros, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado.

AVALIAÇÃO DE RISCOS

A avaliação de riscos orientará na identificação e mensuração de riscos, mitigando-os com a utilização dos controles mais indicados. Constitui um instrumento de identificação de controles que elevem a segurança da informação diante dos pilares de confidencialidade, integridade, disponibilidade e autenticidade.

O objetivo é avaliar as informações do inventário (IDP), identificando as lacunas de segurança da informação e de privacidade sobre os sistemas, demonstrando, à unidade do processo e tomadores de decisão, onde se encontram os riscos dos processos priorizados e o impacto dimensionado, com ações propostas de mitigação destes.

Nesta etapa o foco será:

Identificar e avaliar os riscos

Identificar medidas para tratar os riscos

A seguir são descritos, como exemplo, 14 riscos, com seus respectivos escopos sugeridos para serem utilizados nesta etapa de avaliação.

RISCO	ESCOPO DO RISCO
Acesso não autorizado	Acesso indevido (permissões indevidas) a um ambiente físico ou lógico.
Coleção excessiva	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.
Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	Instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais (LGPD, art. 27).
Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 22 da LGPD.
Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.)	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.
Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma transparente e clara ao detentor dos dados pessoais.
Modificação não autorizada	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.
Perda	Perdas provocadas por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, e provenientes de ações não intencionais como falhas em sistemas, sobrescrita de dados, falhas em hardware, entre outras.
Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento simples de dados pessoais (LGPD, art. 12 e 13)

RISCO	ESCOPO DO RISCO
Remoção não autorizada	Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local.
Retenção prolongada de dados pessoais sem necessidade	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro(a) dos dados pessoais.
Roubo	Dados roubados nas dependências internas do controlador/operador, falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras.
Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Controlador de dados pessoais não obtém consentimento do titular para realizar um tratamento de dados pessoais sem embasamento legal.
Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	A realização de operação de processamento de dados pessoais deve estar em conformidade com a LGPD. Qualquer operação de processamento que não atenda esse requisito pode produzir informações com vinculações ou associações indevidas.

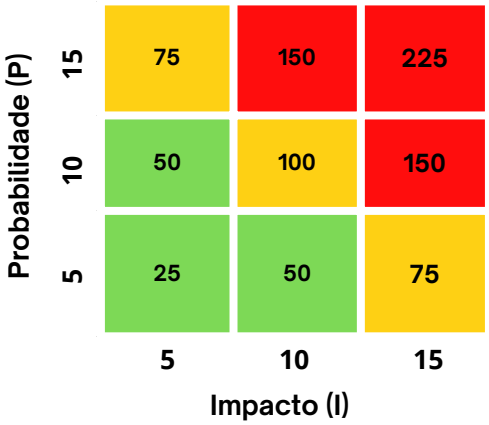
Para cada risco identificado que gere impacto potencial sobre o titular dos dados pessoais, será importante definir:

- a probabilidade de ocorrência do evento de risco;
- o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Como sugestão, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos **níveis de risco** e direcionarão para a aplicação de medidas de segurança.

CLASSIFICAÇÃO	VALOR
BAIXO	**5**
MODERADO	**10**
ALTO	**15**

A figura a seguir apresenta a Matrix Probabilidade X Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco. Nela, o produto da **probabilidade** pelo **impacto** de cada risco deve se enquadrar em uma região (verde, amarela ou vermelha).



Para cada um dos riscos identificados (v. lista dos 14 riscos acima) avalia-se a sua probabilidade de ocorrência, seu impacto e pelo produto desses dois parâmetros, o nível de risco conforme a matriz acima.

Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos.

Impacto: resultado de um evento que afeta os objetivos.

Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades.

Assim, a avaliação de riscos envolve elencar os eventos identificados que afetem o tratamento de dados pessoais, a probabilidade de sua ocorrência, o impacto caso ocorra e, enfim, o nível do risco (probabilidade X impacto).

MEDIDAS DE SEGURANÇA E PRIVACIDADE

A seguir são apresentadas 23 medidas, sendo 12 de segurança e 11 de privacidade, associadas ao objetivo dos controles presentes nela:

Medida de Segurança	Objetivo dos controles presentes na medida de segurança
Continuidade de Negócio	Manter a operação da atividade, apesar das adversidades enfrentadas.
Controles Criptográficos	Oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento).
Controles de Acesso Lógico	Limitar os acessos indevidos ao sistema.
Controles de Segurança em Redes, Proteção Física e do Ambiente	Evitar acessos indevidos às estruturas internas.
Cópia de Segurança	Realizar e manter cópias com temporalidade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais.
Desenvolvimento Seguro	Atender critérios de segurança da informação, desde a concepção do produto.
Gestão de Capacidade e Redundância	Manter a disponibilidade do serviço.
Gestão de Mudanças	Acompanhar as mudanças, comunicar aos interessados e identificar potenciais riscos.
Gestão de Riscos	Identificar, avaliar, gerenciar e monitorar os riscos identificados.
Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	Registrar eventos com atributos de rastreabilidade e proteger de alteração e acessos indevidos.
Resposta a Incidente	Realizar a coleta, a preservação de evidências, o tratamento e a resposta a incidentes de segurança.
Segurança Web	Elevar os níveis de segurança nos serviços de acessos eletrônicos.

Medida de Privacidade	Objetivo dos controles presentes na medida de privacidade
Abertura, Transparência e Notificação	Atender o princípio de transparência da LGPD (art. 6º, inciso VI).
Compliance com a Privacidade	Atender a legislação de proteção de dados, monitorar e auditar a privacidade.
Consentimento e Escolha	Consentimento e Escolha Obter consentimento do titular (art. 7º, I), desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD.
Controles de Acesso e Privacidade	Limitar acessos indevidos às operações de tratamento de dados pessoais (LGPD, art. 6º, Incisos VII e VIII).
Legitimidade e Especificação de Propósito	Realizar tratamento para propósitos legítimos, específicos, explícitos e informados ao titular (LGPD, art. 6º, I)
Limitação da Coleta	Limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6º, III)
Minimização dos Dados	Minimizar os dados utilizados no processamento (LGPD, art. 6º, III)
Participação Individual e Acesso	Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6º, IV)
Precisão e qualidade	Assegurar que os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento (LGPD, art. 6º, V)
Responsabilização	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (LGPD, art. 6º, X).
Uso, Retenção e Limitação de Divulgação	Assegurar aos titulares os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos da LGPD ao realizar o tratamento de dados pessoais.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é documento fundamental e tem por finalidade demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para sua mitigação e que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados (inc. XVII do art. 5º da LGPD).

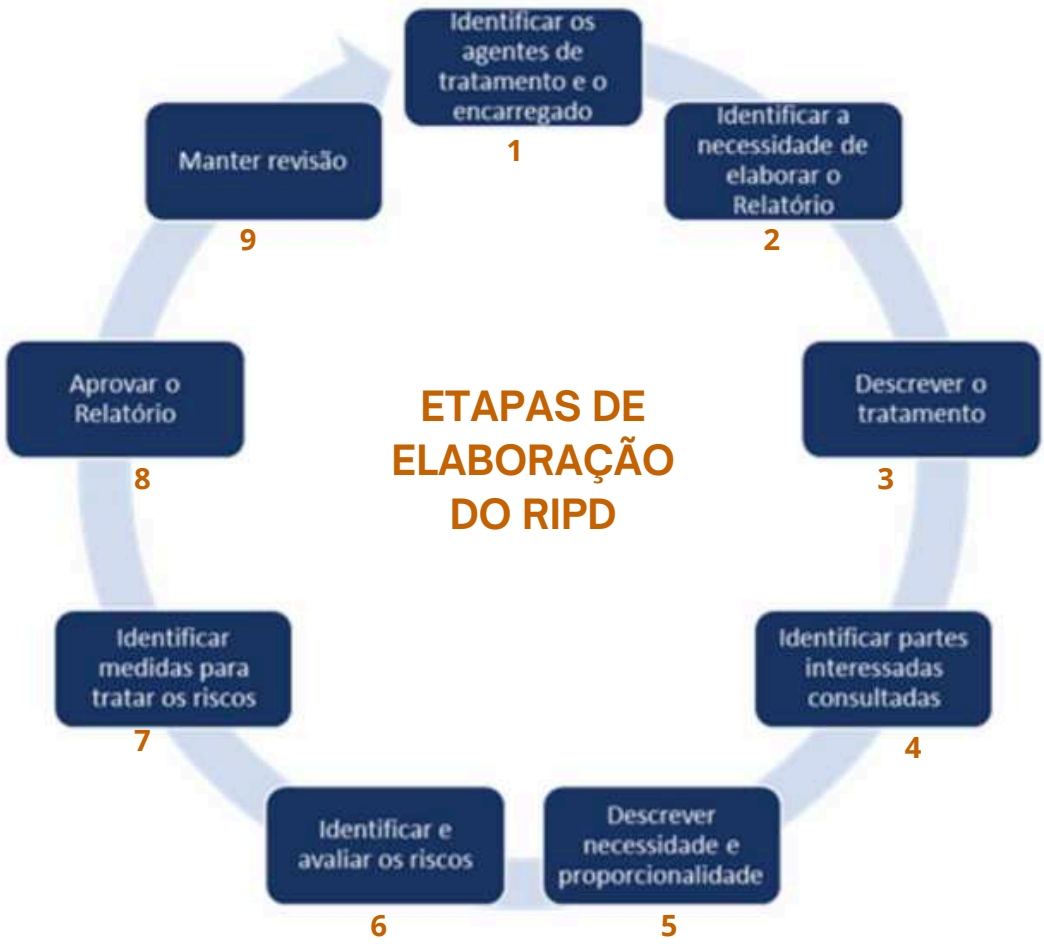
Enquanto o art. 5º inciso XVII define o que é um RIPD, o seu conteúdo mínimo é indicado pelo parágrafo único do art. 38, grifado abaixo.

> *Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.*

Este relatório deverá conter, no mínimo:

- a descrição dos tipos de dados coletados;
- a metodologia utilizada para a coleta;
- a metodologia utilizada para a garantia da segurança das informações; e
- a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O RIPD deve ser elaborado antes de a instituição iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do projeto que tem o propósito de usar esses dados. A elaboração contempla as etapas destacadas pela figura a seguir.



A primeira etapa do RIPD consiste em **identificar os agentes** de tratamento (controlador e operador) e o encarregado no Relatório.

A etapa 2 visa esclarecer a **necessidade de elaboração** do RIPD. Caso seja verificado que o TRT-15 realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode-se optar por um RIPD único. Por outro lado, havendo quantidade expressiva de projetos, sistemas, etc., pode-se considerar a confecção RIPDs segregados.

A etapa 3 refere-se à **descrição do tratamento**, considerando a forma como a instituição pretende tratar o dado pessoal; o escopo que representa a abrangência do tratamento de dados; o contexto que envolve destacar fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais; e a finalidade que é a razão pela qual se deseja tratar os dados pessoais, destacando os resultados e benefícios.

A etapa 4 diz respeito ao **registro das partes interessadas** relevantes, internas e externas, as quais podem ser consultadas a fim de se obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

A etapa 5 identifica as **operações realizadas** sobre os dados pessoais e limitam o tratamento ao mínimo necessário em relação às finalidades (LGPD, art. 6º, III).

A etapa 6 trata da **identificação e avaliação dos riscos** sobre os dados utilizados nas diversas áreas e no conjunto da governança.

A etapa 7 aponta as **medidas para tratar os riscos** que geram impacto potencial sobre o titular dos dados pessoais. Além disso, prevê regras 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 (LGPD, art. 46).

A etapa 8 prevê a **aprovação e formalização do RIPD** por meio da obtenção das assinaturas das partes indicadas como responsáveis pela aprovação do Relatório.

Por fim, a etapa 9 refere-se a revisão do Relatório que deve acontecer anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pelo Tribunal Regional do Trabalho da 15ª Região.

MEDIDAS E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E POLÍTICA DE PRIVACIDADE

Na fase de implementação do **Programa de Governança em Privacidade** tem-se o desenvolvimento e/ou a atualização das diretrizes internas de proteção de dados pessoais. Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes; se é importante a retenção de determinadas informações e se há necessidade de revisão de contratos. Desse modo, torna-se fundamental avaliar a necessidade de uma política de segurança da instituição.

As medidas de segurança para a proteção dos dados pessoais devem ser observadas desde a concepção (*Security by Design*) e a importância de eleger ações preventivas precisam ser consideradas, bem como a gestão dos riscos, a gestão de incidentes e a violação dos dados.

Por fim, mas não menos importante, os direitos dos titulares necessitam ser gerenciados.

ADEQUAÇÃO DE CLÁUSULAS CONTRATUAIS

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento, é importante rever os documentos vigentes e os dados já coletados. No âmbito dos contratos administrativos, pode ser necessário que o Tribunal revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o certame. Pode ser preciso incluir novas cláusulas, conforme os princípios da LGPD (art. 6º).

Como um dos princípios listados é a transparência, torna-se essencial que o contrato apresente informações claras e objetivas, abordando, caso pertinente:

- Delimitações claras e objetivas das responsabilidades do controlador e operador;
- A forma que é realizada a coleta e o tratamento de dados;
- A existência da possibilidade do titular acessar os seus dados coletados;
- A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;

- A existência da possibilidade de revogação do consentimento dado pelo titular;
- O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
- As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

TERMO DE USO

O Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele. O Termo de Uso, como a Política de Privacidade, advém da consciência do controlador e operador serem transparentes com o titular de dados pessoais e comunicarem como as atividades de tratamento desses dados observam o artigo 6º da LGPD.

Em cumprimento aos princípios da publicidade e da transparência, e a fim de assegurar aos cidadãos amplo acesso às informações, os termos devem ser regularmente atualizados de modo a refletir, de forma clara e precisa, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que comumente serão utilizados pelo órgão e entidade no exercício de suas competências legais ou execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

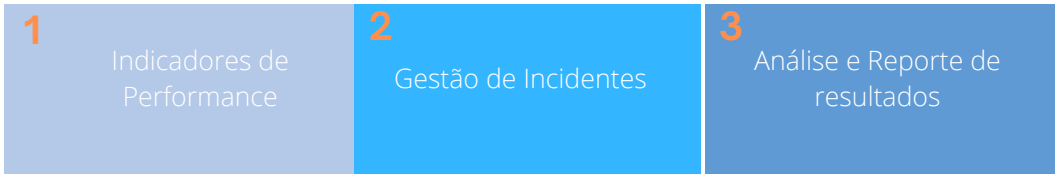
Os tópicos que devem constar no Termo de Uso estão listados a seguir:

1. Aceitação dos Termos e Políticas
2. Definições
3. Arcabouço Legal
4. Descrição do serviço
5. Direitos do usuário
6. Responsabilidades do usuário e da Administração Pública
7. Mudanças no Termo de Uso
8. Informações para contato
9. Foro

MONITORAMENTO

Acompanhar a conformidade da implantação da LGPD é uma atividade contínua e necessária para o Tribunal Regional do Trabalho da 15ª Região manter-se atualizado à legislação a longo prazo e envolve o monitoramento dos planos de ação e medidas recomendadas para adequação, como a correção de fluxos para garantir a minimização das informações e a remoção de dados pessoais que não atendem aos critérios de finalidade de processamento (incluindo *backups*).

A Figura a seguir apresenta os marcos da Etapa de Monitoramento:



INDICADORES DE PERFORMANCE

Os Indicadores de Performance (*Key Performance Indicator* - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no **Programa de Governança em Privacidade**, assim como, o status de outras iniciativas de privacidade.

Sugere-se o uso dos seguintes indicadores:

- Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
- Resultados do Diagnóstico de Adequação à LGPD - índice de adequação;
- Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados / número de serviços com dados pessoais do órgão * 100;
- Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado / quantidade de serviços do órgão * 100;
- Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado / quantidade de serviços do órgão * 100;

- Índice de conscientização em segurança: quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100;
- Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço: quantidade de controles de segurança e privacidade implementados para um determinado serviço / quantidade total de controles de segurança e privacidade identificados para o serviço * 100.

GESTÃO DE INCIDENTES

É importante incluir um processo de Gestão que registre os **incidentes de segurança da informação e de privacidade** ocorridos e que armazene informações como: a descrição dos eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los, a fim de evitar reincidências.

Em caso de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados alguns procedimentos específicos:

- **Avaliar internamente o incidente** com o objetivo de obter informações iniciais sobre impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados; consequências do incidente para os titulares e a entidade, criticidade e probabilidade, além de preservar todas as evidências do incidente.
- **Comunicar ao encarregado** da entidade a existência do incidente, caso envolva dados pessoais.
- **Comunicar ao controlador** (nos termos da LGPD) a existência do incidente, caso envolva dados pessoais.
- **Comunicar à ANPD e ao titular de dados pessoais** (art. 48 da LGPD) a existência do incidente.
- **Comunicar à ETIR** (equipe de tratamento de incidentes cibernéticos internos do Regional), em caso de incidentes na rede computacional.
- **Emitir o relatório final** com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o RIPD.

É válido também implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e respostas a incidentes de segurança da informação e privacidade, de forma a reduzir o nível de risco ao qual o Tribunal está exposto, considerando os critérios de aceitabilidade de riscos definidos pela alta administração.

É recomendado, ainda, que exista um Plano de Comunicação que oriente a forma como os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa.

ANÁLISE E REPORTE DE RESULTADOS

A análise e o reporte de resultados são indicados na etapa de monitoramento para demonstrar o valor do **Programa de Governança em Privacidade** para a alta administração.

Mostrar a evolução das ações e resultados obtidos, assim como o papel da privacidade para o cidadão, fortalece e reforça a cultura de privacidade dos dados. Além disso, auxilia na verificação da necessidade de aprimoramento da Política de Proteção de Dados Pessoais, com a elaboração de normativos complementares.

7 Conclusão

Como vimos, a Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) tem como objetivo assegurar a proteção à privacidade, a transparência, o desenvolvimento econômico e tecnológico, a padronização de normas, a segurança jurídica e o favorecimento à concorrência e a livre atividade econômica.

O Tribunal Regional do Trabalho da 15ª Região, com fulcro na aplicação dos princípios de segurança e prevenção indicados nos incisos VII e VIII do *caput* do art. 6°, da LGPD, considerando sua estrutura, escala e o enorme volume de suas operações; a existência de informações sensíveis tratadas, bem como, a probabilidade e gravidade dos danos para os titulares dos dados, apresenta neste **Programa de Governança em Privacidade**, os passos para o processo de adequação do TRT-15 à nova legislação.

O **Programa de Governança em Privacidade** consolidou as atividades que visam garantir a proteção à privacidade e o cuidado adequado com os dados coletados e tratados, o qual deverá ser atualizado sempre que necessário, de forma a retratar o amadurecimento e desafios institucionais, observando sempre o alinhamento com as diretrizes determinadas pela ANPD.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf> Acesso em 17 de janeiro de 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 17 de janeiro de 2022.

GOVERNO FEDERAL. Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd>.
Acesso em: 10 de janeiro de 2022.

GOVERNO FEDERAL. Guia de elaboração de Programa de Governança em Privacidade (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf>
Acesso em: 15 de janeiro de 2022.

GOVERNO FEDERAL. Guia de Elaboração de Inventário de Dados Pessoais (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf>
Acesso em: 15 de janeiro de 2022.

SECRETARIA DE FINANÇAS DO ESTADO DE RONDÔNIA - SEFIN. Plano de Adequação à Lei Geral de Proteção de Dados - LGPD. Disponível em: <https://www.sefin.ro.gov.br/portalsefin/userfiles/Plano-de-AdequaA%C2%A7A%C2%A3o-A%C2%A0-LGPD-vs-2.pdf>
Acesso em: 14 de janeiro de 2022.

ASSESSORIA DE GESTÃO ESTRATÉGICA
age.presidencia@trt15.jus.br

JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 15ª Região (Campinas)