Tribunal Regional Eleitoral-RN

integração

Programa de Tratamento e Proteção de Dados Pessoais

Versão 1.0 - Abril/2025

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
Abril/2025	1.0	Elaboração do Programa de Governança em Privacidade	ASSINT

LISTA DE ABREVIATURAS E SIGLAS

ANPD - Autoridade Nacional de Proteção de Dados
ASSINT - Assessoria de Integração da Presidência
CPSI - Comissão Permanente de Segurança da Informação
CGPD - Comitê Gestor de Proteção de Dados Pessoais
CNJ - Conselho Nacional de Justiça
ETIR - Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais
ENC - Estratégia Nacional de Cibersegurança da Justiça Eleitoral
ENSEC-PJ - Estratégia Nacional de Segurança Cibernética do Poder Judiciário
GT-SI - Grupo de Trabalho em Segurança da Informação
IDP - Inventário de Dados Pessoais
LAI - Lei de Acesso à Informação
LGPD - Lei Geral de Proteção de Dados Pessoais
PTPD - Programa de Tratamento e Proteção de Dados Pessoais
PSI - Política de Segurança da Informação
RIPD - Relatório de Impacto à Proteção de Dados Pessoais
SSI - Seção de Segurança da Informação
SGP - Secretaria de Gestão de Pessoas
SEI - Sistema Eletrônico de Informações
SGSI - Sistema de Gestão de Segurança da Informação
TRE - Tribunal Regional Eleitoral
TSE - Tribunal Superior Eleitoral

SUMÁRIO

1. INTRODUÇÃO

O **Programa de Tratamento e Proteção de Dados Pessoais (PTPD),** elaborado pelo Tribunal Regional Eleitoral do Rio Grande do Norte (TRE-RN), por intermédio da Assessoria de Integração da Presidência (ASSINT/PRES) e do Comitê Gestor de Proteção de Dados Pessoais (CGPD), envolve a identificação e a integração dos requisitos relacionados à privacidade e à segurança, com o objetivo de orientar e impactar a forma como os dados pessoais são gerenciados ao longo de todo o seu ciclo de vida.

O programa tem fundamento na Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que 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, bem como o livre desenvolvimento da personalidade da pessoa natural, na Resolução n.° 23.650/2021, do Tribunal Superior Eleitoral (TSE), que Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral, e na Resolução n.º 48 do TRE-RN, que dispõe em seu art. 10, inciso III, que compete ao Controlador:

> *III - aprovar o Programa de Tratamento e Proteção de Dados Pessoais, baseando-se em metodologias e instrumentos de governança, gestão de riscos e segurança da informação, a fim de que as ações de tratamento de dados pessoais, durante todo o seu ciclo de vida, sejam permanente e plenamente auditáveis.*

Nesse sentido, o PTPD estabelece diretrizes e práticas que promovem a transparência, as boas práticas, a segurança da informação e o respeito aos direitos dos cidadãos.

O TRE-RN, assim como outras instituições públicas que coletam e processam dados pessoais, deve se adequar à LGPD. Isso implica, entre outras ações, uma transformação cultural dentro da organização, que garanta a incorporação do conceito de privacidade aos ativos de informação e às boas práticas de gestão, de forma que se tornem parte integrante dos processos, sem comprometer sua funcionalidade.

Diante do enorme desafio, o TRE-RN vem procurando preservar a integridade da qualidade do atendimento e do processo eleitoral, buscando alternativas de melhoria contínua, com programas de modernização e excelência operacional, ressaltando a maximização e otimização de resultados e de ferramentas que fundamentam o processo de atendimento ideal aos anseios da sociedade em geral.

Nessa perspectiva, em obediência à Resolução n.º 363, de 12 de janeiro de 2021, do Conselho Nacional de Justiça (CNJ), o TRE-RN inciou, no mesmo ano do referido normativo, ações voltadas para a proteção de dados pessoais, com a instituição do Comitê Gestor de Proteção de Dados Pessoais (CGPD) e o Grupo de Trabalho Técnico, por meio da Portaria n.º 84/2021-GP, revogada e substituída pela Portaria n.º 63/2025/PRES, e com a edição da Resolução TRE-RN n.º 48, de 2021.

Ademais, a LGPD disciplina que os controladores, no âmbito de suas competências, são responsáveis pelo tratamento de dados pessoais e poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização e funcionamento, assim como demais procedimentos relacionados ao tratamento de dados pessoais (conforme a Seção II – Das Boas Práticas e da Governança, do Capítulo VII), tornando-se premente, portanto, a necessidade de elaboração do Programa de Tratamento e Proteção de Dados Pessoais.

Destaca-se, ainda, que o PTPD leva em consideração a estrutura organizacional do TRE-RN e suas especificidades, atuando de forma complementar às ações em andamento, sem substituir demais documentos e atos normativos que disponham sobre o tratamento de dados no âmbito deste Tribunal. Tais ações não apenas fortalecem internamente a instituição, mas também aumentam a confiança da sociedade nos serviços prestados pelo TRE-RN.

Nesse diapasão, o PTPD se aplica a todas as operações de tratamento de dados pessoais realizadas pela Justiça Eleitoral do Rio Grande do Norte, seja por meio físico ou digital. Além disso, o Instrumento se aplica aos(às) magistrados(as), servidores(as) efetivos(as), cedidos(as) e requisitados(as), colaboradores(as) internos(as) e externos(as), estagiários(as), terceirizados(as) e quaisquer outras pessoas que realizem tratamento de dados pessoais em nome da Justiça Eleitoral, de modo que se sujeitam às diretrizes, às normas e aos procedimentos previstos neste programa e são responsáveis por garantir a proteção de dados pessoais a que tenham acesso.

O Programa de Tratamento e Proteção de Dados Pessoais (PTPD) do TRE-RN será atualizado periodicamente para garantir a sua aderência à legislação vigente, às boas práticas de governança e às orientações da Autoridade Nacional de Proteção de Dados (ANPD) e de outros órgãos de controle.

Para assegurar a sua efetividade, a revisão do PTPD ocorrerá, no mínimo, a cada dois anos, ou sempre que houver:

- Alteração relevante na legislação aplicável;
- Publicação de novas normas ou recomendações pelos órgãos reguladores ou fiscalizadores;
- Identificação de mudanças significativas nos processos internos de tratamento de dados pessoais;
- Identificação de riscos relevantes no tratamento de dados pessoais;
- Realização de auditorias internas ou externas que apontem a necessidade de ajustes.

A responsabilidade pela coordenação das revisões caberá à Assessoria de Integração da Presidência (ASSINT) e ao Comitê Gestor de Proteção de Dados Pessoais (CGPD), com o apoio dos setores envolvidos na execução das atividades de tratamento de dados.

2. OBJETIVO

O PTPD tem como objetivo fortalecer a cultura de proteção e tratamento dos dados pessoais dos cidadãos, a fim de melhor orientar e promover a adequação deste Tribunal às diretrizes estabelecidas na LGPD, bem como aos demais instrumentos normativos vigentes para implementação da privacidade e proteção de dados em todas as etapas dos processos de trabalho, com as atualizações necessárias frente a eventuais mudanças normativas e de boas práticas no contexto organizacional.

3. ETAPAS DE IMPLEMENTAÇÃO

A elaboração das etapas do PTPD seguiu o método do ciclo PDCA (Planejar, Executar, Verificar e Agir), baseado nas diretrizes do Guia de Elaboração de Programas de Governança em Privacidade da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia (SGD/ME). O processo foi organizado em três fases, conforme ilustrado a seguir:

Imagem 1 - Etapas de Implementação
Fonte: Autores

3.1 Iniciação e Planejamento

A fase de iniciação e planejamento visa identificar as informações e dados iniciais essenciais para dar início ao planejamento do PTPD. Os principais marcos dessa fase estão definidos da seguinte maneira:

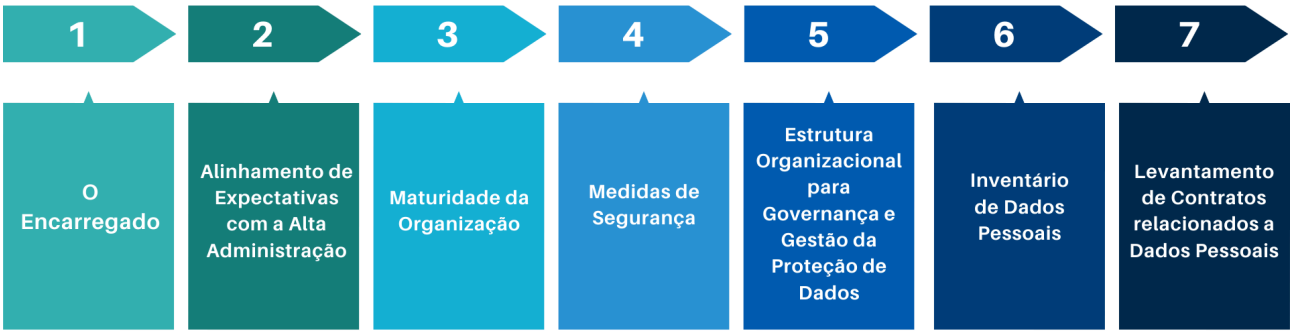

Imagem 2 - Subetapas da Iniciação e Planejamento
Fonte: Autores

3.1.1 O Encarregado

O encarregado tem a responsabilidade de atuar como intermediário entre o controlador, os titulares dos dados e a ANPD. Nesse contexto, em conformidade com o art. 41 da LGPD, o TRE-RN nomeou, por meio da Portaria n.º 84/2021-GP, revogada e substituída pela Portaria n.º 63/2025/PRES, um servidor para a função de Encarregado pelo Tratamento de Dados Pessoais do TRE-RN, ao qual, conforme LGPD, competirá as seguintes responsabilidades:

> *I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;*
>
> *II - receber comunicações da ANPD e adotar providências;*
>
> *III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e*
>
> *IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.*

No exercício de todas as suas atribuições regulamentares, a autoridade designada para a função de Encarregada(o) conta com o apoio do CGPD e com o Grupo de Trabalho Técnico de caráter multidisciplinar, para auxiliar nas funções junto à(ao) Encarregada(o), instituídos pela Portaria n.º 84/2021-GP, revogada e substituída pela Portaria n.º 63/2025/PRES.

Importante ressaltar que o apoio da alta administração é indispensável para o sucesso do trabalho executado pela(o) Encarregada(o), incluindo seu envolvimento nas decisões e recursos suficientes para pessoal, treinamento, entre outros.

A Resolução CNJ n.º 363/2021, em seu art. 1º, estabelece medidas para a adequação dos tribunais à LGPD. Um dos pontos importantes é a criação de um formulário eletrônico ou sistema para o atendimento das requisições e/ou reclamações feitas pelos titulares dos dados pessoais. Essa medida está em conformidade com o item IV, que destaca a responsabilidade dos tribunais em disponibilizar um canal específico, seja diretamente com o encarregado de dados ou em parceria com as ouvidorias dos tribunais, para o devido atendimento das demandas relacionadas à proteção de dados.

Esse formulário eletrônico permitirá que os cidadãos (titulares dos dados pessoais) possam fazer requisições de forma prática e direta, como solicitações de acesso, correção, exclusão ou contestação de dados pessoais, entre outros direitos previstos na LGPD. Além disso, possibilitará o registro de reclamações, que são essenciais para que o Tribunal possa responder de maneira eficiente e transparente, garantindo o cumprimento das disposições legais e o respeito à privacidade dos indivíduos.

Em termos práticos, a implementação desse sistema no sítio eletrônico do Tribunal permitirá a facilitação do processo de adequação à LGPD, promovendo maior transparência e eficiência no tratamento dos dados pessoais dentro do sistema judiciário. Isso também contribuirá para aumentar a confiança dos cidadãos na proteção de seus dados ao interagir com o sistema judicial.

Atualmente, existe um sistema, denominado “fale conosco”, disponível no site do TRE-RN e gerido pela Ouvidoria Eleitoral, por meio do qual o interessado formula seu requerimento e acompanha sua tramitação, inclusive com possibilidade de apresentar recurso. Todavia, hoje o fluxo do requerimento é enviado ao Encarregado via email, no entanto, deve ser comunicado via Sistema Eletrônico de Informações (SEI) enviado pela Ouvidoria Eleitoral.

Importante salientar que o fluxo de tramitação de requerimentos LGPD ainda não foi definido pelo TRE- RN, o que deve ser feito por portaria da Presidência.

3.1.2 Alinhamento de Expectativas com a Alta Administração

O PTPD é fundamental para garantir a conformidade com a legislação de proteção de dados (como a LGPD), e assegurar que a privacidade dos cidadãos e eleitores seja mantida em todos os processos do órgão. Para alinhar as expectativas com a alta administração, é necessário criar um programa estruturado que contemple ações preventivas, monitoramento contínuo e a construção de uma cultura organizacional focada na proteção de dados pessoais.

Dada a relevância do sistema eleitoral para a sociedade brasileira, é de essencial importância que a Política de Proteção da Privacidade seja considerada por todos, da alta administração ao nível operacional. Ou seja, é como uma declaração de comprometimento da alta administração com a privacidade e proteção de dados pessoais, devendo ressaltar a importância de proteger as informações dos cidadãos e a conformidade com as leis vigentes.

Esta etapa representa um passo significativo no processo de início e planejamento do PTPD, pois o alinhamento estratégico com a Alta Gestão é crucial para definir e priorizar ações, visando estabelecer uma cultura de proteção de dados em toda a Organização, com conformidade às boas práticas de governança.

No caso do TRE-RN, já foi elaborada a Política de Tratamento e Proteção de Dados Pessoais, por meio da Resolução n.º 48, de 04 de maio de 2021, um documento que reflete as expectativas da Alta Administração, vez que ela regula a proteção de dados pessoais nas atividades jurisdicionais e administrativas.

Esta política abrange dados pessoais em qualquer formato eletrônico ou físico, cujo tratamento pelo TRE-RN é realizado com o objetivo de atender à sua finalidade pública e promover o interesse público, cumprindo suas atribuições legais e constitucionais.

Conforme estipulado na Política de Tratamento e Proteção de Dados do TRE-RN, o Regimento Interno, o Regulamento Geral e outras normas de organização judiciária e administrativa determinam as funções e atividades que orientam as finalidades e critérios para o tratamento de dados pessoais. Nesse contexto, o Tribunal pode, nas atividades relacionadas diretamente ao exercício de suas competências legais e constitucionais, realizar o tratamento de dados pessoais sem a necessidade de consentimento dos titulares. No entanto, em atividades administrativas que não se vinculam diretamente ao exercício dessas competências, este Tribunal deverá obter o consentimento dos titulares para tratar seus dados pessoais.

3.1.3 Maturidade da Organização

A LGPD entrou em vigor em 18 de setembro de 2020, e as sanções previstas pela lei começaram a ser aplicadas a partir de 1º de agosto de 2021. Durante o processo de adaptação às novas regras, o CNJ emitiu a Recomendação n.º 73/2020, de 20 de agosto de 2020 com o objetivo de incentivar os órgãos do Poder Judiciário a se prepararem para cumprir a nova legislação. Em seguida, foi publicada a Resolução n.º 363/2021, que estabeleceu as medidas que os tribunais devem adotar para garantir a conformidade com as exigências da LGPD.

Importante ressaltar que o nível de maturidade da organização pode ser avaliado por fatores como a rastreabilidade dos dados, a comunicação com os cidadãos e a transparência das ações. O principal objetivo aqui é analisar o estágio atual da instituição em relação à adequação à LGPD.

No intuito de atender à Recomendação n.° 73/2020 e Resolução n° 363/2021, foi elaborado um Plano de Ação, no qual diversas ações de adequação à LGPD foram realizadas (Plano de Ação 2020/2021).

Entre as iniciativas adotadas pelo TRE-RN, destacam-se: a disponibilização de um Portal dedicado à LGPD, com informações sobre a lei, direitos dos titulares, controlador e encarregado de dados pessoais, atos e legislação pertinentes, canal de atendimento, inventário dos dados pessoais tratados e glossário sobre segurança da informação.

Outro ponto importante diz respeito à segurança no processo eleitoral, uma vez que esta é um dos pilares fundamentais para garantir a legitimidade, a transparência e a integridade das eleições. A maturidade do TRE-RN nesse aspecto reflete a capacidade do órgão de proteger, tanto os dados dos eleitores, quanto a infraestrutura dos sistemas eleitorais, além de assegurar a confiabilidade no processo de apuração e divulgação dos resultados.

A maturidade em segurança no processo eleitoral no contexto do TRE-RN pode ser avaliada e desenvolvida por meio de diversos estágios e ações estruturadas, que incluem a implementação de controles, práticas e tecnologias para enfrentar ameaças

cibernéticas, fraudes e outros riscos que possam comprometer a segurança e a confiança nas eleições.

Verifica-se, também, na instituição, o estabelecimento de uma governança de segurança da informação robusta e alinhada aos requisitos de proteção de dados e às melhores práticas de segurança cibernética.

Mais recentemente, por meio da Resolução TRE-RN n.º 106, de 23 de maio de 2023, foi criada a ASSINT/PRES. Dentre suas atribuições, destaca-se a seguinte:

> ***Regulamento da Secretaria (Resolução TRE-RN nº 5/2012)***
>
> *Art. 10-F – À Assessoria de Integração compete prestar assessoramento técnico ao Presidente e, ainda: (Incluído pela Resolução n.º 106, de 23/05/2023)*
>
> *[...]*
>
> *IV - coordenar o Comitê Gestor de Proteção de Dados Pessoais (CGPD), com responsabilidade de cunho estratégico, promovendo as ações necessárias à implantação de mecanismos de tratamento e proteção dos dados pessoais existentes e propondo ações voltadas ao seu aperfeiçoamento; (Incluído pela Resolução n.º 106, de 23/05/2023)*

E, para promover a melhoria contínua e estabelecer padrões que assegurem um ambiente tecnológico seguro e controlado, oferecendo informações essenciais para os processos do Tribunal, com integridade, confidencialidade e disponibilidade, a Política de Segurança da Informação (PSI) do TRE-RN passou por uma recente revisão.

Por fim, importante ressaltar que há um canal de comunicação entre o titular do dado e o TRE-RN, através de *link* disponível na página da *internet*.

3.1.4 Medidas de Segurança

Nessa etapa, devem ser analisadas e adotadas diretrizes, revisando e propondo aprimoramento da cultura interna, tendo em vista o cenário de transformação digital, bem como a necessidade de atendimento ao disposto no *caput* do art. 46 da LGPD, onde resta estabelecido:

> *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.*

Verifica-se, ainda, no § 2º do artigo transcrito, que essas medidas de segurança devem ser observadas desde a fase da concepção até a execução do serviço ou produto. Esse conceito, identificado como *Privacy By Design*, diz respeito ao emprego de meios para preservar a privacidade durante todo o ciclo de vida dos dados pessoais.

Por trás disso, está o pensamento de que a proteção de dados em procedimentos de processamento de dados é melhor respeitada quando já está integrada à tecnologia quando criada. Nesse contexto, o TRE-RN realiza algumas operações de soluções de

proteção do ambiente tecnológico como: *firewall*, antivírus, gerenciamento de acesso, gerenciamento de vulnerabilidades técnicas, dentre outros.

A Resolução TSE nº 23.644, de 1º de julho de 2021, estabelece a Política de Segurança da Informação (PSI) para a Justiça Eleitoral, enquanto a Resolução TRE/RN nº 110/2023, de 10 de agosto de 2023, define a Política de Segurança da Informação específica para o Regional. Ambas as resoluções têm como princípio fundamental assegurar a integridade, a autenticidade, a confidencialidade, a disponibilidade e a irretratabilidade dos ativos de informação e dos processos de tratamento de dados.

Com base nas principais normas orientadoras deste Tribunal, a Comissão Permanente de Segurança da Informação (CPSI), em parceria com a Secretaria de Gestão de Pessoas (SGP), organiza ações de sensibilização durante os eventos de integração de novos servidores, destacando a importância da Segurança da Informação. Em 2017, foram realizados 2 (dois) eventos de integração, nos quais o tema foi abordado; em 2018, ocorreram 4 (quatro) eventos; e, em 2019, foram realizados outros 4 (quatro) eventos. Para o ano de 2020, foi criado um curso na modalidade Educação a Distância (EaD), que substituiu os encontros presenciais, oferecendo aos servidores uma forma mais dinâmica e atualizada de se familiarizar com o tema.

As ações de controle de segurança referentes à proteção de dados no TRE-RN devem ser um conjunto amplo de medidas que tenham como objetivo minimizar os riscos presentes nos ativos de informação.

Alguns informativos veiculados em publicações na *internet, intranet* e no *e-mail* institucional são, também, utilizados com o objetivo de alertar, por exemplo, sobre eventuais ataques de *phishing* (mensagem enviada com o objetivo de obter informações sensíveis, tais como senhas e números de cartões de crédito, para utilização em fraudes) e golpes cibernéticos no *Whatsapp*, inclusive com a realização de curso, pela Escola Judiciária Eleitoral deste Tribunal, tratando sobre *phishing* e segurança da informação.

O Sistema de Gestão de Segurança da Informação (SGSI) do TRE-RN compreende um conjunto de estratégias, diretrizes, políticas, procedimentos, controles e demais mecanismos utilizados para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação. Inicialmente vinculado à Governança Corporativa de Tecnologia da Informação e Comunicação, conforme disposto na Resolução TRE-RN nº 12, de 21 de julho de 2014, o sistema firmou-se como um instrumento fundamental para assegurar que a segurança da informação esteja alinhada aos objetivos e às diretrizes estratégicas da instituição.

É importante salientar que o TRE/RN conta com uma equipe técnica altamente qualificada e estrategicamente estruturada para a gestão da segurança da informação. Essa equipe é composta pela Comissão Permanente de Segurança da Informação (CPSI), instância consultiva e normativa; pela Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR), responsável por ações ágeis e eficazes frente a incidentes; pelo Gestor de Segurança da Informação, profissional especializado e responsável pela articulação das ações de segurança no âmbito institucional; e pela Seção de Segurança da Informação (SSI), unidade técnica vinculada à Coordenadoria de

Infraestrutura Tecnológica/STIE, fortalecida a partir da reestruturação administrativa estabelecida pela Resolução TRE-RN nº 110/2023. Juntas, essas instâncias desempenham um papel fundamental e proativo na preservação da confidencialidade, integridade e disponibilidade das informações no âmbito do Tribunal.

Além disso, conforme estipulado pela Estratégia Nacional de Cibersegurança da Justiça Eleitoral (ENC), o TRE-RN integra a Equipe Nacional de Cibersegurança, sendo representado por um servidor da SSI, unidade vinculada à Coordenadoria de Infraestrutura da Secretaria de Tecnologia da Informação e Eleições (COINF/STIE).

3.1.5 Estrutura Organizacional para Governança e Gestão da Proteção de Dados

A estrutura organizacional para a governança e gestão da proteção de dados pessoais visa apoiar a implementação do PTPD e facilitar as atividades do(a) encarregado(a), que atua como intermediário entre o controlador, os titulares dos dados e a ANPD.

Dessa forma, é essencial que a estrutura seja adequada ao porte da instituição, às suas demandas e competências. Nesse contexto, foi criada a ASSINT – Assessoria de Integração, no âmbito do TRE-RN, com o objetivo de "coordenar o Comitê Gestor de Proteção de Dados Pessoais (CGPD), com responsabilidade de cunho estratégico, promovendo as ações necessárias à implantação de mecanismos de tratamento e proteção dos dados pessoais existentes e propondo ações voltadas ao seu aperfeiçoamento".

O CGPD, por sua vez, é *"responsável pela implementação desta Política e do Programa de* Tratamento *e Proteção de Dados Pessoais, coordena a supervisão das ações de tratamento e proteção de dados pessoais"*, consoante estabelecido no art. 3º, inciso XII, da Resolução TRE-RN n.º 48/2021

Por outro lado, a Governança e Gestão de Tecnologia da Informação e Comunicação, como parte integrante do Sistema de Governança e Gestão da Justiça Eleitoral do Rio Grande do Norte, representa o conjunto estruturado de mecanismos destinados a permitir à alta administração o planejamento, a direção e o controle da utilização atual e futura da TIC, a fim de contribuir para o cumprimento da missão institucional e o alcance dos objetivos estratégicos do TRE-RN.

O Sistema de Gestão de Segurança da Informação do TRE-RN inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. Estabelecido, inicialmente, junto à estrutura de Governança Corporativa de Tecnologia da Informação e Comunicação (Resolução TRE/RN n.º 12/2014), consolida-se como o conjunto de instrumentos estratégicos fundamentais para que a organização possa integrar a segurança da informação às suas políticas e objetivos estratégicos.

Seus objetivos são: instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação; promover ações necessárias à implementação e à manutenção da segurança da informação; combater

atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição; e promover a conscientização e a capacitação de recursos humanos em segurança da informação.

Embasado nas normas NBR ISO/IEC 27001:2006 e NBR ISO/IEC 27002:2006, tem como pilar as Políticas de Segurança da Informação da Justiça Eleitoral e do TRE-RN, que se aplicam a todos os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informação e de processamento no âmbito deste Tribunal.

No TRE-RN, a estrutura de pessoal do SGSI é composta pela CPSI, instituída por meio da Resolução TRE/RN n.º 8/2009, a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR), instituída por meio da Portaria n.º 423/2017, o Gestor de Segurança da Informação, designado através da Portaria DG n.º 45/2017 e, pela Seção de Segurança da Informação (SSI), vinculada à Coordenadoria de Infraestrutura Tecnológica/STIE, criada após reestruturação estabelecida pela Resolução TRE/RN n.º 110/2023.

Além disso, conforme definido pela Estratégia Nacional de Cibersegurança da Justiça Eleitoral (ENC), o TRE-RN faz parte da Equipe de Cibersegurança Nacional, sendo representado por um servidor da Seção de Segurança da Informação (SSI), cujo objetivo é participar de subgrupos formados por outros para conduzir as aquisições de soluções ou serviços de segurança que se façam necessários, bem como de outras iniciativas a partir dos eixos estruturantes da ENC, definidas na Arquitetura de Cibersegurança de referência para a Justiça Eleitoral, elaborada pelo Grupo de Trabalho em Segurança da Informação (GT-SI).

A CPSI (Resolução TRE-RN n.º 8/2009) é responsável por sugerir normas e procedimentos visando à regulamentação e à operacionalização das diretrizes apresentadas na Política de Segurança da Informação vigente, avaliar as mudanças impactantes na exposição dos recursos a riscos, identificando as principais ameaças, analisar criticamente os incidentes de segurança da informação e ações corretivas correlatas, propor iniciativas para aumentar o nível da segurança da informação, promover a divulgação da Política da Segurança da Informação inclusive através de ações educativas, promover processos de gerenciamento de riscos e definir o plano de auditoria periódica, no âmbito do Tribunal e das Zonas Eleitorais. O Presidente da CPSI, designado pela Portaria DG n.º 124/2020, é o Secretário de Tecnologia da Informação e Comunicação, e o suplente, o Coordenador de Infraestrutura Tecnológica.

A mencionada Resolução estabelece as competências da CPSI da seguinte forma:

> *Art. 5º Compete à Comissão Permanente de Segurança da Informação:*
>
> *I - avaliar as mudanças impactantes na exposição dos recursos a riscos, identificando as principais ameaças;*

II - analisar criticamente os incidentes de segurança da informação e ações corretivas correlatas;

III - propor iniciativas para aumentar o nível da segurança da informação;

IV - promover a divulgação da Política da Segurança da Informação, bem como ações para disseminar a cultura em segurança da informação;

V - promover processos de gerenciamento de riscos, bem como a elaboração e aprovação dos planos de continuidade de negócios;

VI - promover ações, com o propósito de viabilizar recursos para o cumprimento da Política da Segurança da Informação;

VII - definir o plano de auditoria periódica, no âmbito do Tribunal e das Zonas Eleitorais.

§ 1º À Comissão compete, ainda, sugerir normas e procedimentos visando à regulamentação e à operacionalização das diretrizes apresentadas na Resolução n.º 22.780, de 24 de abril de 2008, do Tribunal Superior Eleitoral.

§ 2º As normas e procedimentos de que trata o § 1º deste artigo deverão ser elaboradas tomando-se por base os objetivos de controle e controles estabelecidos na NBR ISO IEC 17799:2005, quais sejam:

I - organização da segurança da Informação;

II - gestão de ativos;

III - segurança em recursos humanos;

IV - segurança física e do ambiente;

V - gerenciamento das operações e comunicações;

VI - controles de acessos;

VII - aquisição, desenvolvimento e manutenção de sistemas de informação;

VIII - gestão de incidentes de segurança da informação;

IX - gestão da continuidade do negócio; e

X - conformidade.

Art. 6º Para os efeitos desta Resolução aplicam-se as seguintes definições:

I - usuário: quem utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;

II - recurso: além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

III - atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade fim da Justiça Eleitoral, contemplando todos os ambientes existentes, no âmbito do Tribunal e das Zonas Eleitorais;

IV - segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras

propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas;

V - confidencialidade: a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

VI - integridade: proteção à precisão e à perfeição de recursos;

VII - disponibilidade: a informação será acessível e utilizável sob demanda da entidade autorizada.

A ETIR, instituída por meio da Portaria GP n.º 127, de 27 de agosto de 2020, e vinculada à Secretaria de Tecnologia da Informação deste Tribunal, funcionará como um grupo de trabalho permanente, de atuação primordialmente reativa e não exclusiva. Suas atividades reativas terão prioridade sobre aquelas designadas pelos chefes imediatos de seus respectivos integrantes e tem como objetivo garantir o cumprimento da missão institucional do TRE-RN, por meio do tratamento e resposta a incidentes de segurança na rede interna de computadores.

De acordo com redação dada pela Portaria GP n.º 127/2020, eis as competências da ETIR:

Art. 15. Caberá à ETIR:

I - manter registro dos incidentes de segurança em redes de computadores notificados ou detectados, com o objetivo de assegurar registro histórico das atividades da ETIR;

II - recolher evidências imediatamente após a constatação de um incidente de segurança da informação na rede interna de computadores;

III - executar análise crítica sobre os registros de falha para assegurar que as mesmas foram satisfatoriamente resolvidas;

IV - investigar as causas dos incidentes de segurança da informação na rede interna de computadores;

V - implementar mecanismos para permitir a quantificação e monitorização dos tipos, volumes e custos de incidentes e falhas de funcionamento; e

VI - indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

Dentre os titulares, um deverá ser indicado como Agente Responsável, a quem compete:

Art. 14. Caberá ao Agente Responsável:

I - elaborar os procedimentos internos a serem observados pela ETIR, com apoio da própria equipe;

II - gerenciar as atividades desempenhadas pela ETIR;

III - distribuir, sempre que necessário, tarefas para a ETIR, inclusive as de caráter pró-ativo;

IV - sugerir ao Secretário de Tecnologia da Informação, quando necessário, a convocação de representantes de outras unidades, para atuar no tratamento e resposta de determinado incidente de segurança;

V - assegurar que os usuários sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados;

VI - cuidar da capacitação dos membros da ETIR, fazendo constar do Plano Anual de Capacitação os eventos que entender relevantes ao bom desempenho dos trabalhos da equipe.

De acordo com a Resolução TSE n.º 23.644/2021, compete ao Gestor de Segurança da Informação:

Art. 13. Deverá ser nomeado (Portaria DG n.º 45, de 03/04/2017) um Gestor de Segurança da Informação, no âmbito de cada Tribunal Eleitoral, com as seguintes responsabilidades:

I - propor normas relativas à segurança da informação à Comissão de Segurança da Informação;

II - propor iniciativas para aumentar o nível da segurança da informação à Comissão de Segurança da Informação, com base, inclusive, nos registros armazenados pela ETIR;

III - propor o uso de novas tecnologias na área de segurança da informação;

IV - implantar, em conjunto com as demais áreas, normas, procedimentos, planos ou processos elaborados pela Comissão de Segurança da Informação;

V - acompanhar os processos de Gestão de Riscos em Segurança da Informação e de Gestão de Vulnerabilidades;

VI - definir e acompanhar indicadores de aderência à PSI;

VII - analisar criticamente o andamento dos processos de segurança da informação e apresentar suas considerações à Comissão de Segurança da Informação.

Parágrafo único. O Gestor de Segurança da Informação deverá ser servidor que detenha amplo conhecimento dos processos de negócio do Tribunal e do tema objeto desta Resolução.

Art. 20. A Seção de Segurança da informação e o Gestor de Segurança da Informação apoiarão as demais unidades organizacionais quando da elaboração da análise de riscos de segurança da informação.

Conforme prevê a Portaria GP n.º 127/2020, compete à unidade responsável pela segurança da informação no âmbito do TRE-RN:

Art. 67-H. À Seção de Segurança da Informação compete:

I - promover ações de conscientização sobre segurança da informação;

II - gerenciar a base de conhecimento de serviços de TIC;

III - realizar a análise de vulnerabilidades;

IV - gerenciar o catálogo de serviços de TIC;

V - apoiar o planejamento das contratações quanto às especificações técnicas de microinformática e serviços de TIC;

VI - testar, configurar e homologar os softwares das estações de trabalho que serão disponibilizados aos usuários;

VII - atestar o recebimento, controlar e disponibilizar as licenças de uso de software do Tribunal;

VIII - desenvolver rotinas de automação com objetivo de simplificar a resolução de incidentes pelo próprio usuário;

IX - projetar, customizar, automatizar e implementar adequações às ferramentas de suporte utilizadas pelo Tribunal;

X - oferecer subsídios e operacionalizar a implantação da Política de Segurança da Informação;

XI - gerenciar o processo de incidentes de segurança de TIC;

XII - gerenciar o processo de continuidade de serviços essenciais de TIC;

XIII - mapear e analisar os riscos dos processos críticos da sua área de atuação, inclusive os relacionados à segurança da informação de TIC, e aprimorar ou estabelecer os devidos controles internos para mitigar os riscos identificados;

XIV - elaborar, implantar e acompanhar os processos de trabalho gerenciados pela sua unidade;

XV - fornecer informações e dados relativos a indicadores de desempenho de responsabilidade da unidade, para fins de monitoramento da gestão; e

XVI - desempenhar outras atividades designadas pelo Coordenador, relativas à sua área de competência.

Por meio da Portaria nº 162, de 10 de junho de 2021, o CNJ aprovou os Protocolos e Manuais criados pela Resolução n.º 396/2021, de 7 de junho de 2021, daquele Conselho, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

De acordo com o art. 9º da PSI do TRE-RN (Resolução nº 110/2023), a estrutura normativa da segurança da informação, no âmbito do TRE-RN, será estabelecida e organizada conforme demonstrado a seguir:

I - Nível Estratégico: Política de Segurança da Informação, constituída por esta Resolução, a qual define as diretrizes fundamentais e princípios basilares incorporados pela instituição à sua gestão, de acordo com a visão definida pelo Planejamento Estratégico da Instituição e segundo as orientações da PSI da Justiça Eleitoral.

Atento também à necessidade de aprimoramento contínuo, o TRE-RN promoveu, por meio da CPSI, a atualização da sua Política de Segurança da Informação, que

também integra a estrutura de governança e gestão da proteção de dados pessoais, uma vez que a salvaguarda dos dados pessoais e a segurança da informação estão intrinsecamente associadas.

É importante salientar que a Corregedoria do TRE também tem grande relevância nessa estrutura, conforme dispõe o art. 1º da Resolução n.º 2/1998 do TRE-RN (Regimento Interno da Corregedoria Regional Eleitoral), a seguir:

> *Art. 1º A Corregedoria Regional Eleitoral do Tribunal Regional Eleitoral do Rio Grande do Norte, órgão de fiscalização, disciplina e orientação administrativa, com sede no Tribunal, tem jurisdição em todo o Estado, ficando sob sua supervisão as Zonas Eleitorais e respectivos serviços, bem como os procedimentos para o julgamento dos Processos das atividades correicionais previstas no Regimento Interno e na Lei n.º 4.737/65 – Código Eleitoral.*

Dessa forma, cabe à Corregedoria Regional Eleitoral a orientação e monitoramento acerca do tratamento e proteção de dados pessoais nas Zonas Eleitorais sob sua supervisão.

Além de uma estrutura organizacional clara, é essencial ter normas internas bem definidas para garantir a segurança jurídica e operacional do PTPD. Nesse sentido, a nossa organização tem em sua estrutura as seguintes responsabilidades:

Setor	Responsabilidade na Governança de Privacidade
ASSINT	Treinamento, sensibilização de todos os servidores da Justiça Eleitoral do Rio Grande do Norte e coordenação do CGPD
CGPD	Implementação da Política, coordenação e supervisão das ações de tratamento.
STIE	Implementação de medidas técnicas e segurança cibernética
AJDG, APRES, AJPRES, SAOF, STIE e SGP	Análise de contratos e conformidade regulatória.
Corregedoria	A supervisão da LGPD junto às Zonas Eleitorais
ASCOM	Transparência e Sensibilização

3.1.6 Inventário de Dados Pessoais

O Inventário de Dados Pessoais (IDP) tem como finalidade registrar o tratamento de dados pessoais realizado pela Instituição, conforme o art. 37 da LGPD. Seu objetivo é fazer um levantamento sobre como o TRE-RN lida com os dados pessoais presentes em seus sistemas, identificando os responsáveis pelo tratamento, quais dados são manipulados, onde estão armazenados, quais operações são realizadas com esses dados e outros elementos essenciais para avaliar os riscos e a conformidade com a legislação aplicável.

Ou seja, é a análise do caminho que o dado pessoal percorre desde o momento em que é coletado até o término do tratamento. Assim, permite entender como os dados pessoais são coletados e como se movem pelo órgão.

Esse mapeamento dos dados pessoais tratados pela Instituição é formalizado no IDP, uma ferramenta crucial no processo de rastreamento do tratamento realizado pelo órgão, pois permite identificar os dados processados pelo Tribunal, seus locais de armazenamento e suas finalidades. O processo de classificação da informação desde sua origem deve estar em conformidade com a Lei de Acesso à Informação (LAI) e com a LGPD, especialmente no que se refere aos dados pessoais e sensíveis, sendo um passo essencial para a correta identificação desses dados durante o inventário.

Alguns dados pessoais tratados pelo TRE-RN são considerados confidenciais e só poderão ser acessados por pessoas autorizadas e qualificadas para garantir o tratamento adequado, respeitando as medidas de segurança necessárias para protegê-los contra acessos não autorizados, alterações, divulgação ou destruição dos dados pessoais armazenados.

Em caso de incidente de segurança envolvendo dados pessoais, com risco ou dano significativo, o fato será comunicado à ANPD e ao titular. A comunicação sobre os detalhes do incidente, incluindo sua natureza, os riscos envolvidos, os titulares afetados, as medidas de segurança adotadas e as ações tomadas para o tratamento do incidente será realizada de acordo com o prazo estipulado pela ANPD.

A retenção, o armazenamento ou a eliminação dos dados obedecem à legislação vigente, sem descarte inadequado, em conformidade com as obrigações legais do(a) Encarregado(a).

Dispõe a Resolução n° 363/2021 do CNJ, em seu art. 2º, que, para o cumprimento do disposto na Resolução, recomenda-se que o processo de implementação da LGPD contemple, ao menos, as seguintes ações:

> I – Realização do mapeamento de todas as atividades de tratamento de dados pessoais por meio de questionário, conforme modelo a ser elaborado pelo CNJ.

No entanto, até o momento, não foi realizado o inventário de dados no Tribunal, o que representa uma etapa fundamental para garantir a conformidade com a LGPD. Esse inventário é essencial para identificar quais dados pessoais são tratados, como são processados, quem tem acesso a esses dados e como são armazenados, assegurando que todas as medidas de proteção e controle sejam implementadas corretamente.

3.1.7 Levantamento de Contratos relacionados a Dados Pessoais

Os acordos, contratos e convênios firmados por este Tribunal são monitorados por suas respectivas áreas de atuação, e, em geral, necessitam de um levantamento e análise quanto à conformidade com a LGPD.

Neste Tribunal Regional, passaram a ser utilizadas cláusulas contratuais padronizadas não apenas em novas contratações, mas aos poucos também para

adequação das já vigentes. Além disso, o TRE-RN elaborou um Termo de Confidencialidade, Privacidade e Segurança da Informação a ser utilizado nos contratos firmados entre este Órgão e empresas de prestação de serviço, cujo trabalho demande o acesso a informações de dados pessoais ou informações de outra natureza que devam ser protegidas, para atender à Política de Privacidade e Proteção de Dados Pessoais e às boas práticas de Segurança da Informação.

3.2. Construção e Execução

A segunda etapa consiste na fase de construção e execução, e foram levados em consideração três pontos principais:

> I. Gerenciamento de direitos individuais e fundamentais: O titular possui o direito de acessar seus dados pessoais e também de solicitar sua atualização, correção, anonimização, portabilidade e exclusão, conforme estabelecido no art. 18 da LGPD. Assim, é essencial que o Tribunal realize um gerenciamento adequado dos direitos individuais e fundamentais, estando preparado para receber essas solicitações do titular e atendê-las de maneira satisfatória.
>
> II. Consentimento e rastreabilidade de preferência: O artigo 7º da LGPD estabelece as situações em que é permitido o tratamento de dados pessoais. Embora o tratamento de dados pessoais pelo Poder Público deva ocorrer para cumprir sua finalidade pública, atendendo ao interesse coletivo e buscando executar suas competências ou cumprir suas atribuições legais no serviço público, sendo o consentimento do titular uma exceção, é fundamental facilitar o acompanhamento dos dados tratados pela instituição. Isso deve ser feito de maneira a garantir que o tratamento esteja em conformidade com a LGPD, assegurando a efetivação dos direitos dos titulares previstos na lei.
>
> III. Redução de responsabilidade por violação: Existem medidas para reduzir a exposição dos dados, como a criptografia e a anonimização. Além disso, é importante destacar que a retenção dessas informações deve ocorrer apenas para atender a finalidades específicas. A gestão de riscos de segurança da informação faz parte da área de atuação da SSI e integra o SGSI, sendo responsável por identificar ou propor as medidas de segurança (controles internos) necessárias e adequadas para mitigar os riscos, ajustando-os ao nível aceitável de risco do TRE-RN (apetite ao risco).

Essa etapa se subdividiu nas seguintes fases:

Imagem 3 - Sub etapas da Construção e Planejamento
Fonte: Autores

3.2.1. Políticas e práticas para proteção da privacidade do cidadão e Política de Segurança da Informação

No TRE-RN, a Política de Tratamento e Proteção de Dados Pessoais e a Política de Segurança da Informação orientam as práticas de como o Tribunal lida com dados pessoais, sendo de responsabilidade de todos os seus usuários estarem cientes dessas diretrizes. Para consultá-las, é possível buscar pelos termos “Política de Tratamento e Proteção de Dados Pessoais” (Resolução n.º 48/2021, TRE-RN) e “Política de Segurança da Informação” (Resolução n.º 110/2023, TRE-RN) no Portal do TRE-RN.

3.2.2. Cultura de Segurança de Proteção de Dados e Privacidade desde a Concepção

A LGPD requer a implementação do conceito de *privacy by design,* o qual consiste em um conjunto de boas práticas voltadas a garantir a privacidade desde o início, adotando medidas preventivas e proativas para reduzir riscos, conforme o disposto no art. 46 da referida Lei. Dessa maneira, fomentar uma cultura de segurança e proteção de dados desde sua concepção (*privacy by design*) é uma etapa essencial no desenvolvimento e implementação do Programa de Governança e Privacidade.

Desse modo, deverá ser promovida a conscientização para disseminar a cultura de proteção da privacidade desde a criação e ao longo de todo o ciclo de vida da informação, destacando-se a comunicação do PTPD, com o objetivo de alcançar uma privacidade por padrão, por meio da adoção de boas práticas, como a definição clara da finalidade, limitação na coleta e no uso dos dados, além de critérios para retenção e divulgação, entre outros.

Merecem destaque alguns valores desse modelo, a seguir:

I - a proatividade e não reatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema para evitar a ocorrência dos riscos de privacidade;

II - a incorporação de controles de privacidade, oferecendo o máximo grau de privacidade que serão auditados e avaliados continuamente, sendo parte integrante do sistema, sem diminuir a funcionalidade;

III - a visibilidade e transparência, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos com confiança; e

IV - o respeito pela privacidade do usuário que deve ser alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que forneçam autonomia ao titular dos dados.

3.2.3. Relatório de Impacto à Proteção de Dados Pessoais

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é um instrumento fundamental para avaliação da conformidade do tratamento de dados pessoais em relação à LGPD. Um dos objetivos do RIPD é descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como de análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

A elaboração de um RIPD tem por objetivo descrever as operações de tratamento de dados pessoais realizadas pelo Tribunal, com foco na avaliação dos riscos que essas operações podem apresentar aos direitos e liberdades dos titulares de dados. Este relatório também deverá apresentar as medidas adotadas pelo TRE-RN para mitigar os riscos identificados, em conformidade com a LGPD e as orientações da ANPD.

O relatório deve abranger, igualmente, as ações, proteções e mecanismos para redução de riscos, conforme previsto nos arts. 5º, inciso XVII, e 38, 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, transcrito 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.*

Destaca-se, ainda, que o art. 4º da Resolução nº 2/2022 da ANPD descreve que o tratamento de dados será considerado de alto risco se envolver situações como "larga escala", uso de dados sensíveis, decisões automatizadas, entre outros.

O art. 6º da LGPD exige que os controladores considerem o alto risco e as medidas de mitigação ao elaborar o RIPD.

Este relatório deverá conter, no mínimo:

- A descrição dos tipos de dados coletados:

- Dados de identificação pessoal: nome, CPF, RG, data de nascimento, etc;
- Dados de contato: e-mail, telefone;
- Dados sensíveis: informações sobre saúde, filiação político-partidária, dados de vulnerabilidade, biometria, entre outros, quando aplicável;
- Entre outros.

- A metodologia usada para os diversos tipos de tratamento, tais como:

  - Gestão eleitoral: identificação de eleitores, alistamento eleitoral, revisão eleitoral, organização de eleições, apuração e divulgação de resultados;
  - Gestão de servidores e colaboradores: processos de admissão, pagamento e administração de recursos humanos;
  - Gestão de contratos: aquisições de bens e serviços e contratos;
  - Gestão de processos judiciais e administrativos: Pje e SEI;
  - Atendimento ao público: interação com cidadãos, respondendo a demandas e solicitações;
  - Cumprimento de obrigações legais: emissão de certidões eleitorais, registros de candidaturas e resultados eleitorais;
  - Entre outros.

- A metodologia utilizada para a garantia da segurança das informações:

  - Armazenamento seguro: dados são armazenados de forma criptografada em servidores com acesso restrito;
  - Segregação de dados: as informações pessoais são tratadas separadamente para garantir que apenas os responsáveis por determinadas funções tenham acesso aos dados necessários para o cumprimento de suas responsabilidades;
  - Controle de acesso: políticas de controle de acesso são implementadas para garantir que apenas usuários autorizados possam acessar dados sensíveis.

- A análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Com base nos critérios da LGPD, as operações de tratamento realizadas pelo TRE-RN serão avaliadas quanto ao risco que podem apresentar para os direitos e liberdades dos titulares dos dados. A seguir, são apresentadas as principais medidas adotadas para mitigar esses riscos:

- Risco de acesso não autorizado: utilização de criptografia, controle de acesso com autenticação multifatorial e auditorias periódicas.
- Risco de vazamento de dados pessoais sensíveis: implementação de políticas de acesso restrito, treinamentos contínuos sobre segurança e privacidade, e comunicação eficiente de incidentes de segurança.

- Risco de discriminação ou prejuízos aos direitos dos titulares: adoção de mecanismos de transparência e direitos dos titulares, como a possibilidade de acesso, retificação e exclusão dos dados.

Além disso, em situações de risco elevado, o TRE-RN deverá adotar as seguintes ações adicionais:

- Implementação de medidas preventivas, como a anonimização ou pseudonimização de dados, sempre que possível.
- Adoção de tecnologias emergentes e inovadoras com cautela, quando aplicável, respeitando os princípios da LGPD.

O RIPD deve ser elaborado antes de a Instituição iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do projeto que tenha o propósito de usar esses dados.

Assim, dispõe a ANPD sobre o RIPD:

> *É importante que o relatório seja suficientemente detalhado, para que a ANPD e o próprio controlador tenham compreensão ampla de como ocorre o tratamento dos dados pessoais e os possíveis riscos associados a ele.*
>
> *Assim, recomenda-se ao controlador descrever os tipos de dados pessoais tratados, as operações de tratamento (art. 5º, X, da LGPD), suas finalidades (incluindo interesses legítimos) e hipóteses legais, e avaliar a necessidade e a proporcionalidade das operações de tratamento, os riscos para os direitos e liberdades dos titulares de dados e as medidas a serem adotadas para minimizar esses riscos.*
>
> *Embora a divulgação do RIPD não seja, em regra, obrigatória, permitir o acesso ao público em geral pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas, previstos, respectivamente, pelo art. 6º, incisos IV, VI e X, da LGPD.*
>
> *Para isso, o controlador pode disponibilizar o RIPD em meios de fácil acesso pelo titular, especialmente em seus sítios eletrônicos, com informações sobre suas atividades de tratamento de dados pessoais, de forma clara, adequada e ostensiva.*
>
> *Contudo, nesse caso a versão pública do RIPD pode ser distinta da versão interna, no intuito de resguardar segredos comercial e industrial e outras informações protegidas por lei.*
>
> *Especificamente em relação a entidades e órgãos públicos, o RIPD deverá ser publicado: (i) por determinação da ANPD, nos termos do art. 32 da LGPD; ou (ii) pelo próprio controlador, quando não identificada hipótese de sigilo aplicável ao caso, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011.*

Enquanto não for editado regulamento específico sobre o RIPD, os controladores podem, no que couber, adotar como parâmetro o conceito de tratamento de alto risco definido no art. 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução nº 2/2022.

De acordo com esse dispositivo, o tratamento será de alto risco se verificada, no caso concreto, a presença de, ao menos, um critério geral ("larga escala" ou "afetar significativamente interesses e direitos fundamentais dos titulares") e de um critério específico ("uso de tecnologias emergentes ou inovadoras", "vigilância ou controle de zonas acessíveis ao público", "decisões tomadas unicamente com base em tratamento automatizado de dados pessoais" ou "utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos").

Considerando esses critérios, recomenda-se elaborar o RIPD, por exemplo, se o tratamento de dados pessoais abranger número significativo de titulares ("larga escala", critério geral) e dados pessoais sensíveis (critério específico). Outro exemplo que pode ser mencionado é a decisão tomada unicamente com base em tratamento automatizado de dados pessoais (critério específico), da qual possa resultar a negativa para o exercício de um direito ou para a utilização de um serviço ("afetar significativamente interesses e direitos", critério geral).

Ressalte-se que, para fins de elaboração do RIPD, esses critérios não devem ser considerados exaustivos, de modo que o controlador poderá verificar a existência de alto risco em situações diferentes das indicadas. Assim, em conformidade com o princípio da responsabilização e prestação de contas, cabe ao controlador avaliar as circunstâncias relevantes do caso concreto, a fim de identificar os riscos envolvidos e as medidas de prevenção e segurança apropriadas, considerando os possíveis impactos às liberdades e direitos fundamentais dos titulares e a probabilidade de sua ocorrência.

É importante salientar que o controlador do tratamento de dados pessoais no TRE-RN é o próprio Tribunal Regional Eleitoral do Rio Grande do Norte, responsável pela coleta, tratamento, armazenamento e compartilhamento de dados pessoais, conforme as finalidades legais e institucionais previstas.

Os processos de tratamento de dados pessoais precisam ser descritos no RIPD de forma a permitir que o titular e demais partes interessadas compreendam o processo e, também, implementem medidas para mitigar os riscos.

Nesse contexto, o RIPD deverá ser desenvolvido pelo TRE-RN, por meio da(o) Encarregada(o) de Dados e pelo setor de Segurança da Informação, quando as operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.

3.2.4. Adequação das Cláusulas Contratuais

Os contratos e convênios que envolvem o tratamento de dados pessoais devem estar em conformidade com a LGPD. Para aqueles firmados antes da vigência da lei, é necessário realizar ajustes para assegurar, por um lado, a proteção dos dados pessoais e, por outro, garantir a transparência, oferecendo informações claras e objetivas sobre a forma como o tratamento é realizado e assegurando que o titular tenha acesso aos seus dados.

Nesse contexto, o TRE-RN implementou mudanças nos contratos existentes, para adequá-los à LGPD, e passou a adotar, como norma, a assinatura do Termo de Confidencialidade, Privacidade e Segurança por contratados e/ou colaboradores, sempre que o contrato envolver o acesso a dados pessoais ou outras informações que exijam proteção e preservação.

Além disso, é imprescindível que se faça o levantamento dos contratos vigentes pelas unidades responsáveis, com o objetivo de promover a adequação daqueles que ainda não possuem cláusulas de proteção conforme as diretrizes da LGPD.

3.2.5. Política de Tratamento e Proteção de Dados

Importante ressaltar que a Resolução CNJ n.° 363/2021, ao dispor sobre o estabelecimento de medidas de adequação à LGPD, ressaltou a necessidade de:

> *Art. 1º […]*
>
> *[...]*
>
> *VI – disponibilizar informação adequada sobre o tratamento de dados pessoais, nos termos do art. 9º da LGPD, por meio de:*
>
> *a) avisos de cookies no portal institucional de cada tribunal;*
>
> *b) política de privacidade para navegação na página da instituição;*
>
> *c) política geral de privacidade e proteção de dados pessoais a ser aplicada internamente no âmbito de cada tribunal e supervisionada pelo CGPD;*
>
> *[..]*

Nesse sentido, o TRE-RN elaborou a Política de Tratamento e Proteção de Dados do TRE-RN que foi editada através da Resolução n.º 48, de 04 de maio de 2021.

3.2.6. Política de Privacidade

A Política de Privacidade é um documento essencial que descreve como coleta, usa, armazena e compartilha os dados pessoais de seus usuários, clientes, colaboradores e qualquer outra pessoa que interaja com seus sistemas. Isso inclui tanto informações fornecidas diretamente pelos usuários (como formulários preenchidos), quanto dados coletados automaticamente, como por meio de *cookies* e outras tecnologias.

É um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece

privacidade ao usuário, cumprindo, fundamentalmente, o dever de transparência, disposto como princípio na LGPD. Trata-se aqui de uma política de privacidade externa, que faz parte do Termo de Uso, também podendo ser chamada de “aviso de privacidade” que fornecerá às pessoas externas à Organização um aviso sobre as práticas de privacidade adotadas, bem como outras informações relevantes.

Como já dito anteriormente, ter uma Política de Privacidade é uma exigência da Resolução CNJ n.° 363/2021.

Um dos princípios dessa lei é o consentimento do titular dos dados, ou seja, a pessoa deve autorizar a coleta e o uso de seus dados pessoais, embora a maioria dos dados tratados pelo TRE-RN seja para o exercício de atribuições legais ou execução de políticas públicas. Todavia, quando há necessidade de consentimento, este deverá ser informado, ou seja, a pessoa precisa entender claramente como seus dados serão tratados.

A principal função da Política de Privacidade é informar o usuário sobre como seus dados serão coletados, usados, processados e armazenados. Ela deve esclarecer quem terá acesso a essas informações, quais medidas de segurança estão em vigor, o que acontece em caso de vazamento de dados, por quanto tempo os dados serão mantidos e quem é o Encarregado de Proteção de Dados, responsável pela gestão e proteção dessas informações na Instituição.

Além disso, é importante que a Política de Privacidade seja clara, acessível e de fácil entendimento. Ela não deve estar escondida em páginas difíceis de encontrar nem escrita de forma complicada. O objetivo é garantir que o usuário tenha acesso fácil e rápido às informações sobre o tratamento de seus dados. (ANEXO I – Política de Privacidade do Portal do TRE-RN)

Os requisitos básicos para a elaboração da Política de Privacidade são:

> I - definições da Política de Privacidade: A Política de Privacidade deve ser acessível, com linguagem clara e fácil de entender para todos os usuários, sem termos técnicos complicados, a fim de garantir transparência no tratamento dos dados pessoais;
>
> II - base legal para tratamento de dados pessoais: a hipótese de tratamento de dados pessoais autorizada pela LGPD, bem como sua previsão legal devem ser informadas ao titular dos dados.

Assim, tratando-se de um Tribunal responsável por administrar as eleições, o tratamento dos dados pelo TRE-RN encontra respaldo nos arts. 7º e 11 da LGPD, no que se refere ao tratamento de dados para cumprimento de obrigação legal ou regulatória pelo controlador e tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;

> III - Controlador, Operador e Encarregado: o titular dos dados tem direito de acesso às informações de contato do controlador, que deverão ser disponibilizadas de forma clara, adequada e ostensiva, contendo a identificação, endereço e

informações de contato do controlador, que nesse caso é o TRE-RN. Da mesma forma, deve ser informado que os dados do Encarregado constam no sítio eletrônico do TRE-RN e restar claro que dúvidas podem ser sanadas pelos canais devidos;

IV - direitos do titular dos dados pessoais: toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

Assim, visando o princípio da transparência, numa Política de Privacidade, devem ser informados os direitos de seus titulares, especialmente aqueles descritos nos arts. 9º e 18 da LGPD;

V - tratamento dos dados e sua finalidade: é realizado pelo TRE-RN para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as suas atribuições do serviço público. Assim, deve restar claro na Política de Privacidade quais dados serão tratados e qual sua finalidade. Os principais tratamentos de dados realizados pelo TRE-RN estão relacionados à **gestão eleitoral:** identificação de eleitores, alistamento eleitoral, revisão eleitoral, organização de eleições, apuração e divulgação de resultados; **gestão de servidores e colaboradores:** processos de admissão, pagamento e administração de recursos humanos; **gestão de contratos:** aquisições de bens e serviços e contratos; **gestão de processos judiciais e administrativos:** Pje e SEI; **atendimento ao público:** interação com cidadãos, respondendo a demandas e solicitações; **cumprimento de obrigações legais:** emissão de certidões eleitorais, registros de candidaturas e resultados eleitorais; **segurança institucional:** coleta de dados para identificar pessoas que ingressam em suas dependências e nelas transitam; e **cadastro e registro:** credenciamento de usuários para utilização de sistemas administrativos e judiciais. O tratamento das informações se destina, como regra, à análise, concessão e manutenção de benefícios. No entanto, outros dados poderão ser tratados e devem ser igualmente informados. Destaca-se nessa seção o atendimento aos princípios estabelecidos no art. 6º da LGPD, especialmente o princípio da necessidade, que estabelece a limitação do tratamento ao mínimo necessário para a realização das finalidades previstas, de forma proporcional e não excessiva;

VI - coleta dos dados: além de especificar quais dados são coletados, é importante esclarecer ao titular como os dados são obtidos. Os dados mais relevantes para o reconhecimento de direitos vêm do cadastro eleitoral e PJe, que são bases de dados onde estão armazenadas as informações eleitorais e processuais. Todavia, outras bases de dados, inclusive de outros órgãos, podem ser utilizadas. Pode, ainda, haver coleta de informações por meio de funcionalidades específicas do dispositivo do usuário como, por exemplo, pela câmera, para dados de biometria;

VII - compartilhamento de dados: para estar em conformidade com a LGPD, o serviço deverá informar ao titular do dado que utiliza o serviço sobre o uso

compartilhado de dados pelo controlador e a finalidade de seu compartilhamento. Ao realizar o compartilhamento dos dados, deverá sempre ser observada a inclusão de cláusulas de preservação de sigilo das informações;

VIII - transferência internacional de dados: para os casos que envolvam transferência de dados entre países, deve-se deixar claro para o titular quais os dados serão transferidos internacionalmente, para qual finalidade, quais países estão envolvidos e qual o grau de proteção e privacidade fornecido por eles;

IX - segurança dos dados: é fundamental que sejam apresentadas ao titular dos dados as medidas de segurança que foram implementadas no serviço que trata seus dados pessoais, além de definir meios para que seja comunicado sobre a ocorrência de incidente de segurança que lhe possa acarretar risco ou dano relevante. Também é importante citar qual o canal de comunicação para que o titular reporte possíveis violações, falhas e vulnerabilidades do serviço, que esteja em consonância com o Plano de Gestão de Incidentes Cibernéticos ou outros planos que venham a ser elaborados;

X - *cookies*: a sua utilização deve considerar a hipótese legal que considere a prévia autorização do usuário ou qualquer outra hipótese que respalde a coleta desses dados, devendo estar claro o aviso sobre sua utilização, consentimento e informar a respeito de quais dados pessoais são coletados, armazenados e para qual finalidade;

XI - tratamento posterior dos dados para outras finalidades: deve ser comunicado ao titular do dado, informando-o a respeito de quais dados poderão ser utilizados para tratamentos posteriores e qual a sua finalidade.; e

XII - mudanças na Política de Privacidade: a política poderá ser alterada a qualquer momento para atender à evolução do serviço oferecido ou à LGPD. Por isso, recomenda-se que seja informada ao usuário a forma de comunicação das mudanças realizadas, sua versão atual e a data da última atualização do documento. Deverão ainda ser mantidas informações das datas de vigor e teor das versões anteriores.

3.2.7. Plano de conscientização, treinamento e comunicação

Para que um PTPD seja bem-sucedido em sua implementação, é crucial que toda a Organização esteja devidamente alinhada. Uma forma eficaz de disseminar conhecimento é por meio de programas de capacitação e sensibilização dos(as) magistradas(os), servidoras(os), colaboradores, estagiárias(os), sem esquecer que planos de comunicação devem ser constantemente aprimorados.

As campanhas de capacitação e comunicação devem informar sobre as legislações e políticas relevantes, as sanções em caso de violação e estimular a utilização dos canais de denúncia, com a devida divulgação desses meios.

O plano de sensibilização, treinamento e comunicação:

I - incluirá um cronograma regular de cursos com certificação, abordando temas relacionados aos direitos de privacidade e proteção de dados pessoais, como segurança da informação, direito à privacidade e gestão de riscos; e

II - abrangerá a criação de materiais, atualizados de forma periódica, com diretrizes e normas de boas práticas relacionadas à segurança da informação, disponibilizados a todos os colaboradores, além de ações para promover a incorporação da cultura de proteção de dados pessoais nas unidades do TRE-RN.

3.3. Monitoramento

O monitoramento é a última etapa do PTPD e consiste no processo de acompanhamento das fases que o antecedem, objetivando verificar se as medidas implementadas estão de acordo com o instituído no PTPD e as recomendações emitidas nos RIPDs, bem como se aquelas medidas foram suficientes para conformidade do tratamento de dados à LGPD e, ainda, para solucionar a situação apontada nos relatórios como inadequada frente aos critérios adotados.

Imagem 4 - Sub etapas do Monitoramento
Fonte: Autores

3.3.1. Indicadores de performance

Os indicadores de performance devem procurar avaliar o nível de conformidade do TRE-RN em relação à LGPD. Para isso, é necessário contar com ferramentas e métodos que possibilitem a medição das ações de proteção à privacidade já implementadas, com o objetivo de acompanhar o progresso das áreas no processo de adaptação dos serviços e sistemas, além de verificar se as medidas adotadas são adequadas e cumprem os requisitos de proteção dos dados. Assim, pode ser realizada anualmente e abranger a avaliação dos índices de:

I - maturidade, a ser realizado através do Diagnóstico de Adequação à LGPD;

II - internalização institucional referente à LGPD, o qual poderá ser mensurado por meio de formulários elaborados e aplicados nas diversas etapas - implantação, pós campanha de comunicação, pós capacitação; e

III - adequação de acordos, contratos e convênios à LGPD.

O objetivo de um indicador é ajudar a monitorar o progresso do Tribunal em relação à implementação da LGPD e permitir a identificação de áreas que precisam de melhorias, garantindo a conformidade com a legislação e a proteção adequada dos dados pessoais, de modo que um indicador deverá ser regulamentado por meio de uma portaria da presidência.

3.3.2 Gestão de Incidentes

Um incidente de segurança envolvendo dados pessoais é qualquer evento negativo confirmado, originado por um ato intencional ou acidental, relacionado a uma falha na segurança dos dados pessoais, que leve à divulgação, modificação, destruição ou perda indevida desses dados, além de acessos não autorizados ou qualquer forma de tratamento inadequado ou ilegal de dados, independentemente do meio de armazenamento, comprometendo a confidencialidade, integridade ou disponibilidade das informações pessoais.

Para a eficiência da Gestão de Incidentes é imprescindível a definição dos atores, papéis e responsabilidades, sejam individuais ou coletivos, além da elaboração e divulgação de fluxos com a descrição das atividades de tratamento de incidentes.

O que foi bem definido na PSI e no SGSI do TRE-RN que inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Importante mencionar que a criação de normas relacionadas à Gestão de Incidentes deve ser baseada na clareza das informações, na definição precisa das responsabilidades dos envolvidos, no alinhamento técnico com a operadora e na elaboração de um escopo e objetivos que sejam facilmente compreendidos por todos.

Além dos incidentes de natureza cibernética, existem outros que também podem afetar a privacidade no tratamento dos dados pessoais. O vazamento de dados é um dos incidentes de segurança mais conhecidos, ocorrendo quando informações são acessadas, coletadas, divulgadas ou transmitidas a terceiros de maneira inadequada. Os danos ao titular podem variar, incluindo fraudes, tentativas de golpes, uso indevido das informações, venda de dados, entre outros.

Nos casos de incidentes de segurança que não envolvam necessariamente a tecnologia da informação, deverá ser elaborado um plano de resposta, definindo fluxos, papéis e responsabilidades, levando em conta também as diretrizes da ANPD e outros regulamentos aplicáveis.

A Gestão de Incidentes de privacidade deve consistir, portanto, na recepção, tratamento e resposta a esses incidentes, buscando identificar sua causa raiz, documentar e avaliar os riscos que afetem as operações de tratamento de dados pessoais.

Por fim, é fundamental incluir a Gestão de Incidentes na etapa de Monitoramento para que estes eventos fiquem registrados com as informações e sistemas envolvidos,

medidas técnicas e de segurança utilizadas para a proteção das informações, riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências.

Portanto, faz-se necessário, também, implementar controles e procedimentos de forma a reduzir o nível de risco ao qual a Instituição está exposta, além do que, deve-se incluir um plano de comunicação tanto para os órgãos fiscalizadores, quanto para a imprensa.

Existem, ainda, alguns procedimentos específicos que precisam ser adotados em caso de incidente de violação de dados pessoais, descritos a seguir:

- Ante a constatação da ocorrência do incidente, caso envolva dados pessoais, aquela deverá ser comunicada à(ao) Encarregada(o) e ao(à) representante do Controlador;
- A(O) representante do controlador comunicará a ocorrência do incidente, em prazo razoável, à ANPD e ao titular de dados pessoais, nos termos do art. 48 da LGPD;
- Caso seja determinado pela ANPD, ante uma maior gravidade do incidente, o Controlador dará ampla divulgação do fato em meios de comunicação, adotando medidas para reverter ou mitigar os efeitos do incidente, nos termos do § 2º do art. 48;
- Constatando-se a real gravidade do incidente, podem ser necessárias medidas que tornem os dados pessoais afetados ininteligíveis;
- Emissão de relatório com as informações sobre o incidente, ações realizadas e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o RIPD, dentro da política de mitigação de riscos.

Para a Gestão de Incidentes, o TRE-RN desenhou seu processo, por meio da Portaria GP n.º 236, de 12 de dezembro de 2023, em alinhamento com o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário, estabelecido pelo CNJ. É importante destacar o papel do usuário na comunicação e reporte de potenciais incidentes.

3.3.3 Análise e Reporte de Resultados

A Análise e o Relatório de Resultados fazem parte da fase de monitoramento, com o objetivo de evidenciar à Alta Administração o valor do PTPD e são essenciais para o fortalecimento da cultura de privacidade dos dados, além de mostrar o progresso das ações realizadas e seus resultados. Vale destacar que a privacidade é de extrema importância para o cidadão, desempenhando um papel fundamental no fortalecimento da cultura de proteção de dados. Portanto, é essencial apresentar a evolução das ações e os resultados alcançados, o que reforça a cultura de privacidade de dados dentro da Instituição e auxilia na identificação de oportunidades para aprimorar a Política de Proteção de Dados Pessoais.

4. COMUNICAÇÃO E TRANSPARÊNCIA

A LGPD estabelece a possibilidade de criar regras de boas práticas de governança para aprimorar as ações que promovam e reforcem a proteção dos direitos fundamentais de dados, liberdade, privacidade e o pleno desenvolvimento da personalidade da pessoa natural. Dentro desse contexto, um Plano de Comunicação tem como objetivo apresentar, a todos os envolvidos, as principais ações e estratégias adotadas por este Tribunal Regional no âmbito do PTPD.

Nesse sentido, destacam-se as principais iniciativas de governança, alinhadas com as boas práticas organizacionais deste Tribunal, de ação contínua, realizadas e a realizar:

- Criar um portal dedicado à LGPD (realizada);
- Criar canais de comunicação para que os cidadãos possam exercer seus direitos sobre os dados pessoais (ação contínua);
- Alinhar as expectativas com a alta Administração (ação contínua);
- Melhorar a maturidade da Organização (ação contínua);
- Adotar Medidas de Seguranças (ação contínua);
- Adequar Estrutura Organizacional voltada para a Governança e Gestão de Proteção de Dados Pessoais (ação contínua);
- Realizar o Inventário de Dados Pessoais (IDP) (a realizar)
- Disseminar a Cultura de segurança e proteção de dados pessoais e *privacy by design* (ação contínua);
- Publicar Relatório de Impacto à Proteção de Dados Pessoais (RIPD) dos processos realizados (a realizar);
- Adequar as cláusulas contratuais (realizadas, alguns contratos anteriores 2023, a realizar);
- Elaborar Indicadores de Performance - medir e comunicar o desempenho do Órgão (a realizar);
- Elaborar Política de Privacidade e Política de Segurança da informação (realizada);
- Elaborar Política de Tratamento e Proteção de Dados Pessoais (realizada);
- Promover a Gestão de Incidentes (ação contínua);
- Publicar relatórios anuais sobre a implementação do PTPD, incluindo estatísticas sobre o tratamento de dados e incidentes de segurança (ação contínua).

5. CONCLUSÃO

A LGPD visa garantir a proteção dos direitos fundamentais de liberdade, privacidade e o pleno desenvolvimento da personalidade da pessoa natural.

Com esse propósito, o PTPD do TRE-RN foi desenvolvido com o objetivo de orientar as atividades que assegurem a proteção à privacidade, em conformidade com a LGPD, refletindo o nível de maturidade da instituição e os desafios a serem enfrentados, sempre em estrita observância às diretrizes estabelecidas pela ANPD e pelo CNJ.

Com isso, o TRE-RN se compromete a proteger os dados pessoais tratados em suas operações, garantindo a privacidade e a segurança das informações dos cidadãos. Este PTPD será um instrumento fundamental para construir um ambiente de confiança e responsabilidade.

Por fim, é importante destacar que o Tribunal pode estabelecer acordos de cooperação técnica com outras instituições e entidades, com o objetivo de alcançar as metas e objetivos descritos neste Programa. Esses acordos podem envolver diversas áreas, como segurança da informação, tecnologia da informação, capacitação de recursos humanos, e outras ações estratégicas que fortaleçam as iniciativas do Tribunal em conformidade com as diretrizes estabelecidas.

Esses acordos são uma ferramenta essencial para promover a troca de conhecimentos, recursos e melhores práticas entre organizações, permitindo o desenvolvimento de soluções mais eficientes e eficazes. Além disso, a cooperação técnica pode viabilizar a implementação de projetos conjuntos, a realização de treinamentos especializados, a atualização de sistemas, a integração de novas tecnologias e a adoção de normas e processos mais robustos.

Por meio dessas parcerias, o Tribunal pode ampliar sua capacidade de atender às exigências legais e técnicas relacionadas à segurança da informação, fortalecer sua infraestrutura tecnológica e garantir a proteção dos dados e ativos da Justiça Eleitoral, sempre com foco na melhoria contínua dos serviços prestados à sociedade.

Por fim, este PTPD será efetivado por meio da elaboração de Plano de Ação Bienal a ser aprovado mediante Portaria da Presidência do TRE-RN.

6. REFERÊNCIAS

BRASIL. Lei n° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: jan. 2025.

BRASIL. Lei n° 12.965, de 23 de abril de 2014 - Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: jan. 2025.

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: mar. 2025.

BRASIL, Tribunal Regional Eleitoral do Rio Grande do Norte. Ato Portaria GP TRE-RN n.º 127, de 27 de agosto de 2020 (alteradora). [Altera a Portaria n.º 423/2017-GP, que [Institui a Equipe de Tratamento e Resposta Incidentes em Redes Computacionais (ETIR) no âmbito do TRE/RN]. Disponível em: https://www.tre-rn.jus.br/legislacao/legislacao-compilada/portarias-gp/portarias-gp-por-a

no/2020/portarias-2020-1/tre-rn-portaria-gp-n-o-127-de-27-de-agosto-de-2020-alteradora. Acesso em: mar. 2025.

BRASIL, Tribunal Regional Eleitoral do Rio Grande do Norte. Ato PTRE-RN Resolução n.º 110, de 10 de agosto de 2023. [Institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte]. Disponível em: https://www.tre-rn.jus.br/legislacao/legislacao-compilada/resolucoes-do-tre-rn/resolucoes-por-ano/2023/tre-rn-resolucao-n-o-110-de-10-de-agosto-de-2023. Acesso em: mar. 2025.

GOVERNO FEDERAL. Comitê Central de Governança de Dados - CCGD. Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias/guia_lgpd.pdf. Acesso em: mar. 2025.

GOVERNO FEDERAL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia de elaboração do Programa de Governança em Privacidade (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: fev. 2025.

BRASIL, Tribunal Regional Eleitoral do Rio Grande do Norte. Ato TRE-RN Resolução n.º 48, de 04 de maio de 2021. [Altera a Portaria n.º 423/2017-GP, que [Institui a Política de Tratamento e Proteção de Dados Pessoais no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte]. Disponível em: https://www.tre-rn.jus.br/legislacao/legislacao-compilada/resolucoes-do-tre-rn/resolucoes-por-ano/2021/tre-rn-resolucao-n-o-48-de-04-de-maio-de-2021. Acesso em: mar. 2025.

BRASIL. Conselho Nacional de Justiça. Resolução nº 363, de 12 de janeiro de 2021. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: fev. 2025.

BRASIL. Conselho Nacional de Justiça. Recomendação nº 73, de 17 de junho de 2020. Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições da Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.cnj.jus.br/recomendacao-orienta-tribunais-sobre-protecao-de-dados/. Acesso em: fev. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD Nº 18, de 16 de julho de 2024. Disponível em: Acesso em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: fev. 2025.

BRASIL. Tribunal Regional do Trabalho da 5ª Região. Programa de Governança em Privacidade. Salvador: TRT5, 2022. Disponível em: https://www.trt5.jus.br/sites/default/files/www/lgpd/programa_de_governanca_em_privacidade_trt5.pdf. Acesso em: fev. 2025.

ANEXO I – Política de Privacidade do Portal do TRE-RN

Política de Privacidade de Dados

O Tribunal Regional Eleitoral do Estado do Rio Grande do Norte TRE-RN adota as práticas necessárias para garantir a segurança e a privacidade das informações pessoais coletadas de seus usuários que acessam o portal do Tribunal, em conformidade com a legislação vigente, incluindo a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Esta Política de Privacidade descreve como coletamos, usamos, armazenamos, protegemos e compartilhamos seus dados pessoais, bem como os direitos que você tem sobre suas informações e é complementar à Política de Tratamento e Proteção de Dados Pessoais (Resolução n.º 48/2021, TRE-RN).

1. Aceitação da Política

Ao acessar ou utilizar nossos serviços, você declara que leu, compreendeu e concorda com os termos desta Política de Privacidade. Caso não concorde com alguma das disposições aqui descritas, você deverá interromper o acesso aos nossos sites e aplicativos.

2. Base legal para tratamento de dados pessoais

Tratando-se de um Tribunal, responsável por administrar as eleições, o tratamento dos dados pelo TRE-RN encontra respaldo nos arts. 7º e 11 da LGPD, no que se refere ao tratamento de dados para cumprimento de obrigação legal ou regulatória pelo controlador e tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos.

Nesse contexto, o Tribunal pode, nas atividades relacionadas diretamente ao exercício de suas competências legais e constitucionais, realizar o tratamento de dados pessoais sem a necessidade de consentimento dos titulares. No entanto, em atividades administrativas que não se vinculam diretamente ao exercício dessas competências, este Tribunal deverá obter o consentimento dos titulares para tratar seus dados pessoais.

3. Coleta de Dados Pessoais

A coleta de dados pessoais ocorre quando você acessa nossos portais e aplicativos ou utiliza os serviços prestados. Os dados podem ser coletados de forma voluntária ou automática. Os dados pessoais que podemos coletar incluem, mas não se limitam a:

- Informações de identificação (nome, CPF, endereço, e-mail, telefone);

- Dados de navegação (IP, tipo de navegador, sistema operacional, páginas acessadas, tempo de navegação);
- Dados fornecidos durante o cadastro ou utilização de serviços específicos.

4. Uso dos Dados Pessoais

Os dados pessoais coletados serão utilizados para os seguintes fins:

- Prestação dos serviços solicitados, como consultas, agendamentos ou outros serviços relacionados;
- Melhoria da experiência do usuário, através de análises estatísticas e aprimoramento dos serviços;
- Cumprimento de obrigações legais e regulamentares.

5. Armazenamento de Dados

Os dados pessoais serão armazenados de maneira segura em nossos sistemas, de acordo com as boas práticas de segurança da informação. O acesso a essas informações será restrito a profissionais autorizados que necessitem delas para a execução de suas funções.

5. Cookies e Tecnologias de Rastreamento

Utilizamos cookies e tecnologias similares para melhorar a experiência de navegação do usuário, coletando informações como o endereço IP, o tipo de navegador, páginas visitadas e o tempo de acesso. Esses dados são utilizados para fins estatísticos, melhorias na funcionalidade do site e para personalizar o conteúdo. O usuário pode optar por desabilitar os cookies em seu navegador, mas isso pode afetar a funcionalidade de alguns serviços.

6. Compartilhamento de Dados Pessoais

Seus dados pessoais poderão ser compartilhados com terceiros apenas nas seguintes situações:

- Com parceiros, prestadores de serviços e empresas contratadas que auxiliam na execução dos serviços oferecidos pelo TRE-RN;
- Quando exigido por força de lei ou por decisão judicial;
- Quando houver seu consentimento expresso para o compartilhamento.

7. Segurança da Informação

O TRE-RN adota medidas de segurança para proteger seus dados pessoais contra acesso não autorizado, alteração, divulgação ou destruição. Contudo, nenhuma medida de segurança é completamente eficaz, e não podemos garantir a segurança total de seus dados em todas as circunstâncias.

8. Direitos do Titular dos Dados

Você tem os seguintes direitos sobre seus dados pessoais:

- Acesso: direito de consultar os dados pessoais que possuímos sobre você;
- Correção: direito de corrigir dados pessoais incorretos ou desatualizados;
- Confirmação: de que existe um ou mais tratamento de dados sendo realizado;
- Eliminação: direito de solicitar a exclusão de seus dados pessoais, salvo se houver obrigação legal de mantê-los;
- Informação sobre compartilhamento: de seus dados com entes públicos e privados, caso exista;
- Portabilidade: direito de solicitar seus dados pessoais em formato estruturado, para transferência a outro serviço;
- Reclamação: contra o controlador dos dados junto à autoridade nacional;
- Revogação do consentimento: direito de revogar a qualquer momento o consentimento dado para o tratamento de seus dados.

Para exercer seus direitos, entre em contato com o encarregado de proteção de dados pessoais do TRE-RN através do e-mail [encarregado@tre-rn.jus.br].

9. Links para Outros Sites

O portal do TRE-RN pode conter links para outros sites de terceiros. Não nos responsabilizamos pela política de privacidade ou pelo conteúdo desses sites. Recomendamos que você leia as políticas de privacidade desses sites antes de fornecer qualquer dado pessoal.

10. Alterações na Política de Privacidade

Esta Política de Privacidade poderá ser atualizada a qualquer momento. Recomendamos que você a consulte regularmente para se manter informado sobre como estamos protegendo seus dados pessoais. A data da última atualização será sempre indicada no final do documento.

11. Contato

Se você tiver dúvidas sobre esta Política de Privacidade ou sobre o tratamento de seus dados pessoais, entre em contato com o encarregado de proteção de dados pessoais do TRE-RN através do e-mail [encarregado@tre-rn.jus.br].