PROJETO LGPD TJPB

Relatório Final

Projeto

Juiz Auxiliar Responsável: Dr. Meales Melo

Coordenação

Projeto: Ana Carolina Leal
Tecnologia da Informação: José Teixeira de Carvalho Neto
Negócios: Rossana Guerra de Sousa
Jurídico: Rodrigo Antonio Nóbrega

Equipe

Tecnologia da Informação:
Raphael de Almeida Porto
Anderson Rodrigues Ribeiro

Negócios:
Eudes Moacir Toscano Júnior
Amilton Costa Gomes

Jurídico:
Mário Zenaide

Início : 14.01.2020
Final: 30.07.2020

ROTEIRO

Introdução

O TJPB inicia seu percurso rumo à implementação do Programa de Proteção de Dados Pessoais a partir de um projeto para cumprimento dos requisitos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), iniciado em janeiro de 2020, com a constituição de força tarefa composta por representantes da área de negócios, jurídica e de tecnologia da informação.

Como resultado do trabalho dessa força tarefa, foram definidos conceitos, critérios e metodologias para possibilitar a realização do diagnóstico inicial da gestão de dados pessoais, a análise das lacunas de conformidade e a análise de risco dos processos. Adicionalmente, também foi apresentada proposta de Política para gestão da LGPD no âmbito do TJPB.

Munido de todo esse material, o Encarregado de Dados Pessoais conseguirá trilhar o caminho rumo a evolução do nível de maturidade da gestão da LGPD no TJPB. A produção de todo esse conhecimento o auxiliará também na tomada de decisão, na execução dos planos de ações e demais ajustes necessários para assegurar a conformidade requerida pela norma.

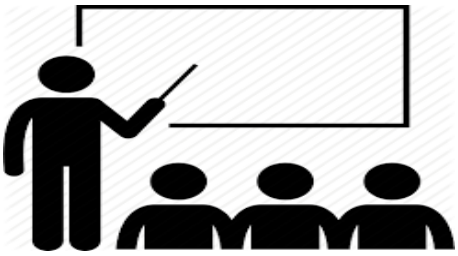
A seguir, descrever-se-ão os conceitos, critérios e metodologias utilizadas pela força tarefa para realização do mapeamento de dados, cujo diagnóstico inicial compõe o Relatório de Análise de Dados Pessoais (RADP) e se constitui na ferramenta inicial para o Programa de Proteção de Dados Pessoais do TJPB, com a nomeação e atividade do Encarregado Geral de Proteção de Dados.

Fases do Projeto LGPD

Responsável: Equipe de Projeto

Objetivo: Preparação (avaliação e desenho) das operações e Organização das estruturas e mecanismos para possibilitar a implementação dos requisitos da LGPD no TJPB pelo DPO

Registros - Atas

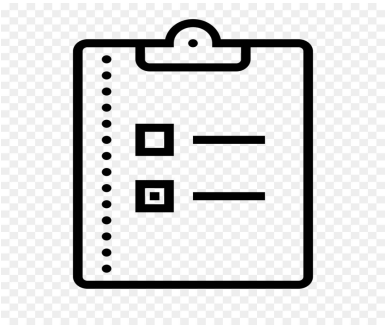


1. **Conscientização**
    a. Levantamento de requisitos e necessidades - Proposta inicial;
    b. Sensibilização e apoio da alta administração;
    c. Definição do grupo de trabalho;
    d. Conscientização e conhecimento sobre dados e parâmetros da LGPD - Capacitação da equipe inicial do Projeto e áreas estratégicas - Consultor Fabiano Castello;

2. **Projeto, Desenho e Metodologia**
    a. EAP Projeto - EAP Projeto
    b. Definição de:
        i. áreas estratégicas para o projeto
        ii. papéis das equipes (Negócios, Tecnologia e Jurídico) e suas atribuições;

iii. conceitos e taxonomias;
iv. metodologia para: coleta e análise de lacunas legais e de governança, mapeamento do fluxo de dados; identificação e análise de riscos;
v. modelos para registro estruturado das atividades de tratamento;

c. Preparação dos instrumentos de esclarecimento iniciais sobre dados e LGPD;
d. Preparação e validação dos instrumentos para coleta estruturada e entrevistas;
e. Elaboração do modelo estrutural para Relatório de Análise de Dados (RAD) para consolidar o mapeamento de dados (artigo 37) e possibilitar a demonstração do nível de exposição e auxiliar na evolução do nível de maturidade do TJPB.
f. Definição de acompanhamento do projeto pela Gerência de Projetos TJPB.



3. Mapeamento do Fluxo de Dados e Segurança da Informação

a. Levantamento e mapeamento com questionário e entrevistas, do ciclo de vida e do fluxo de dados pela equipe de negócios diretamente com as áreas;
b. Levantamento, a partir do fluxo de dados de negócios, do inventário de ativos e avaliação de segurança da informação pela equipe de tecnologia;
c. Identificação de estrutura de dados pela equipe de tecnologia;

4. **Documentação, Identificação e Análise de Riscos e Lacunas**
    a. Documentação - Relatório de de Análise de Dados (RAD) - equipe de negócios e TI;
    b. Recomendação e validação das bases legais pela equipe jurídica;
    c. Classificação das lacunas de conformidade e de governança e LGPD;
    d. Classificação dos riscos de cada processo;
    e. Identificação dos terceiros críticos por processo;

5. **Governança de Proteção de Dados**
    a. Revisões e adequações contratuais - equipe jurídico;
    b. Identificação e proposta de Framework para acompanhamento da maturidade;
    c. Elaboração de minuta de Política de Proteção de Dados Pessoais;

d. Elaboração de material audiovisual para capacitação de servidores e magistrados quanto a conceitos e importância da LGPD para o TJPB;
e. Proposta de fases para Programa de Proteção de Dados Pessoais e Privacidade.
f. Definição dos agentes de tratamento;
g. Desenvolvimento de hotsite com informações sobre LGPD no âmbito do TJBP.

Fases para Programa de Proteção de Dados Pessoais e Privacidade - Proposta

Responsável: Alta Administração e Encarregado de Proteção de Dados
Objetivo: Implementar e monitorar as operações necessárias para a implementação dos requisitos da LGPD no TJPB

1. Plano de Ação e Maturidade da Governança de Proteção de Dados

a. Estabelecer a partir do RAD o atual nível de maturidade e governança dos processos de proteção de dados do TJPB;

2. Estabelecer, com base nos riscos, o plano de ação necessário, com seus respectivos responsáveis e prazos para migrar os riscos e evoluir para o próximo nível de maturidade desejado;
3. Definir com base em riscos a necessidade do DPIA;
4. Propor a estrutura de governança de dados.

2. Regulamentação e Gestão

a. ***Ações de Regulação*** - propostas para administração :

i. Programa de Proteção de Dados e Privacidade
ii. Políticas de privacidade TJPB;
iii. Políticas e procedimentos para Privacy by Design nos projetos do TJPB;
iv. Manual Básico da LGPD do TJPB
v. Plano de comunicação, conscientização e treinamento sobre Proteção de dados e privacidade

vi. Plano de comunicação para questões Proteção de dados e Privacidade
vii. Orçamento e estrutura necessária para Gestão de Proteção de Dados;

b. ***Ações de Estruturação de Segurança da Informação*** - propostas com a área de TI
   i. Sistema para classificação, aprovação de processamento e registro de bancos de dados que contenham dados pessoais;
   ii. Controles de segurança para dados pessoais.
   iii. Informações da coleta, finalidade, política de cookies etc.
   iv. Procedimentos para manutenção de avisos de privacidade de dados;

c. ***Ações de Gerenciamento*** LGPD
   i. Plano e registros de direito dos titulares de dados, tratamento de solicitações, reclamações e retificações de dados.
   ii. Procedimentos e periodicidade para avaliação de riscos e gerenciamento
   iii. Periodicidade de atualização dos relatórios de análise de dados pessoais
   iv. Plano de resposta à violação de privacidade e vazamento de dados pessoais
   v. Sistema informatizado para gerenciamento de Proteção de Dados e Privacidade
   vi. Estratégia de anonimização de dados nas fontes

d. Ações de Monitoramento
   i. Sistemática de auto avaliação de controles para as áreas envolvidas no processo de proteção de dados e privacidade;
   ii. Auditoria interna de conformidade e gestão sobre adequação LGPD;
   iii. Auditoria externa certificadora

Áreas Estratégicas

As áreas e atividades estratégicas foram definidas a partir do conhecimento geral do negócio central do TJPB.

Para o ordenamento de sua relevância para o projeto foram considerados os seguintes parâmetros: sensibilidade, criticidade e abrangência da atividade quanto a utilização e proteção de dados pessoais e privacidade.

Os parâmetros de avaliação variam de 1- muito baixo a 5 muito alto;

Quadro 1- Atividades de Processamento Estratégicas - Escolhar

Área	**Atividade de Processamento**	SENSIBILIDADE	CRITICIDADE	ABRANGÊNCIA	ORDEM
Diretoria de Gestão de Pessoas	Cadastro de Servidores, Magistrados, Estagiários e Leigos	5	5	5	125
Corregedoria	Cadastro de Notariais, Selo, Sare	4	4	4	64
Segurança	Sistema de Monitoramento de Câmeras	5	4	3	60
Segurança	Controle de Acesso	5	5	2	50
Diretoria de Economia e Finanças	Precatórios	4	4	3	48
Diretoria Administrativa	Contratação	4	4	3	48
Diretoria Administrativa	Contratação- Licitação				
Diretoria de Gestão de Pessoas	Qualidade de Vida	3	4	3	36
Diretoria	Locação de	3	4	2	24

Administrativa	Terceirizados				
Diretoria de Gestão de Pessoas	Cessão de Mão de Obra	2	3	3	18
Diretoria Administrativa	Engenharia	4	2	2	16
Comunicação	Arquivo	1	3	5	15
Diretoria de Economia e Finanças	SIAF	1	4	2	8
Jurídica/Judiciária/1º Grau	Processo Judicial	1	5	1	5
ESMA	Sistema de Ensino	2	2	1	4
Segurança	Base de Autoridades	1	3	1	3
Comunicação	Certidões	2	1	1	2
Comunicação	Matérias Jornalísticas	1	1	1	1
Comunicação	Diário da Justiça	1	1	1	1
Comunicação	Reclamações	1	1	1	1
Comunicação	Biblioteca	1	1	1	1
Diretoria de Economia e Finanças	Adiantamento	1	1	1	1
Diretoria de Gestão de Pessoas	Peritos, tradutores, intérpretes e leiloeiros	1	1	1	1
Diretoria Administrativa	Chamados	1	1	1	1

Conceitos e Taxonomias

Para possibilitar um entendimento comum entre as equipes do projeto, foram definidos conceitos e classificações para utilização na fase de coleta de dados para diagnóstico.

Dados Pessoais - Categorias
Nome
Data Nascimento
Filiação
Dados de Descendentes
Sexo
Naturalidade
Fotografias / imagens em vídeo
Nome usuário nas redes sociais
Estado Civil
Cônjuge
Endereço
Telefone
e mail
Profissão
RG
CPF
PIS
CNH
Carteira ProfissionaL
Título de Eleitor
Passaporte
Matrícula

Local de Trabalho
Salário
Cargo
Data de Posse
Dados Bancários
Dado acadêmico
Registro Profissional

Titular de Dado
Servidor
Magistrado
Estagiário
Juiz Leigo
Voluntário
Perito ou tradutor
Familiares de servidor/magistrado
Terceirizados
Representante de contratado ou licitante
Notário
Visitante ou convidado
Transeunte
Aluno não servidor
Parte
Licitante

Dados Sensíveis
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
Dado penal, criminal ou tributário

Origem dos dados
Diretamente do titular
Outra área de atividade de tratamento
Provedor externo

Agentes Responsáveis pelo Tratamento
Controlador
Operador

Métodos de Transferências
E-mail institucional
E-mail não institucional
Aplicativos de mensagens
Aplicação de Integração - API
Formulário web
Formulário em papel
Cópia eletrônica por e-mail
Transferência de arquivos
Telefone
Serviços web
Não sabe informar
Aplicação de Integração - AP e e mail

Transferência para entidades Privadas
Execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI;
Se for indicado um encarregado para as operações de tratamento de dados pessoais;
Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (que deverão ser comunicados à autoridade nacional);
Para a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados;
Nos casos em que os dados forem acessíveis publicamente;
Outros não relacionados.

Nível de Interesse na Intrusão
1 - Baixo, dados públicos facilmente acessíveis;
2 - Médio dados que podem possibilitar uso para cadastros ou divulgação externa;
3 - Alto, dados que podem ser usados para fins de manipulação de comportamento, dados de crédito ou dados sensíveis

Parâmetros de prazo e forma para tratamento
Prazo indeterminado para guarda de dados pessoais sensíveis;
Prazo indeterminado para guarda de dados pessoais em geral;
Falta de consentimento para dados de menores;
Transferência de dados por aplicativos de mensagem ou e mail não institucionais;
Utilização de planilhas pessoais para armazenamento e tratamento de dados pessoais sem proteção da organização;
Documentos físicos armazenados sem proteção ou procedimento

específico;
Bases de dados pessoais sem proteção para manuseio, download, tratamento;
Transferência de dados pessoais para terceiros sem proteção direta ou regulação;
Dados passados para atividades analíticas com acesso a outras áreas na organização;
Consentimento sem condições do artigo 8º e 9º;
Base legal de legítimo interesse não cobre o disposto no artigo 10.

Base Legal
Art. 7º, I - mediante fornecimento de consentimento pelo titular;
Art 7º II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
Art 7º 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;
Art. 7º 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;
Art. 7º 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);
Art. 7º VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
Art. 7º VIII -para a tutela da saúde exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
Art 7º IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais - apoio e promoção de atividades do controlador;

Art 7º IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais;
Art 7º X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;
Não há dados sensíveis;
Art. 11 I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
Art. 11 II, a - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para a) cumprimento de obrigação legal ou regulatória pelo controlador;
Art. 11 II, b - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
Art. 11 II, c - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para c) realização de estudos por órgão de pesquisa, garantida, sempre que possível,a anonimização dos dados pessoais sensíveis;
Art. 11 II, d - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para o 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
Art. 11 II, e - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para e) proteção da vida ou da incolumidade física do titular ou de terceiro;
Art. 11 II, f - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para 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) Vigência

Art. 11 II, g - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para 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.

Compartilhamento dos dados
Outras entidades externas do Poder Público
Outras entidades externas privadas
Contratados privados
Convênios de Compartilhamento Público

Retenção de dados
Até 05 anos
Até 20 anos
20 anos após o desligamento do servidor
20 anos ou mais
Prazo indeterminado
Até 01 ano
Não sabe informar

Avaliação do nível de segurança de sistemas
Não há medidas de segurança ou medidas ad hoc
Medidas reativas ou apenas políticas organizacionais não institucionalizadas
Medidas reativas, organizacionais ou preventivas institucionalizadas
Medidas preventivas, reativas e políticas organizacionais institucionalizadas
Medidas preventivas, reativas e políticas organizacionais institucionalizadas e gerenciadas

Finalidade do tratamento dos dados
Art. 4º - II - realizado para fins exclusivamente: a) jornalístico e artísticos e /ou b) acadêmicos;
Art. 4º -III - Realizado para fins exclusivos de:a) segurança pública;
Art. 4º -III - Realizado para fins exclusivos de: b) defesa nacional;
Art. 4º -III - Realizado para fins exclusivos de: c) segurança do Estado;
Art. 4º -III - Realizado para fins exclusivos de: d) atividades de investigação e repressão de infrações penais;
Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público,

Coleta de Dados - Formulário

A coleta de dados foi realizada a partir de questões formatadas e consolidadas em formulário constante do link:

https://docs.google.com/spreadsheets/d/1nZMmzQV6QzvJs1RhRSTOrufugjUQjl1dvByBxlI3k64/edit?usp=sharing

O formulário de coleta foi aplicado eletronicamente e as respostas analisadas, ajustadas e validadas com a área respondente.

Fluxo de Dados - Metodologia de Registro

O fluxo de dados foi mapeado usado a metodologia de Diagrama de Fluxo de Dados constante do link:
https://drive.google.com/file/d/1zgTWnAvtXYBn5rOMsKB_Umc7oq2ilUaz/view?usp=sharing

Identificação e Análise de Riscos - Dicionário de Riscos e Gap Analysis

Para o estabelecimento de políticas e salvaguardas deve ser utilizado um processo de avaliação sistemática de impactos e riscos à privacidade, nos termos do disposto no artigo 50, letra d, § 2º da Lei 13.709/2018.

Para possibilitar a identificação e avaliação dos riscos à privacidade, e na ausência de metodologia padronizada por órgão regulador, foi definida pela força tarefa do projeto a sistemática, para análise de riscos e identificar lacunas de conformidade e governança que possam impactar no objetivo do processo, a partir dos seguintes conceitos:

Risco - a possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos (COSO ICIF 2013), avaliado através da combinação entre a probabilidade de ocorrência de um evento (aleatório e futuro) e o impacto (negativo) que este evento possa ter na consecução do objetivo do processo.

Risco Inerente – é o risco ao qual uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco Residual –é o risco ao qual uma organização está exposta após considerar as ações de mitigação aplicadas para reduzir a probabilidade de sua ocorrência ou seu impacto, ou ambos.

Apetite a Risco – o nível de risco que a organização está disposta a aceitar enquanto persegue seus objetivos

Respostas a Riscos – envolve a escolha de opções de ações para gestão do risco identificado. Pode ser categorizada em: aceitar, mitigar, compartilhar ou evitar.

Matriz de Riscos – ferramenta de gerenciamento de riscos que permite identificar de forma visual os riscos a que a organização está sujeita.

Parâmetros escalares para avaliação de riscos:

1	Muito Baixo
2	Baixo
3	Médio
4	Alto
5	Extremo

Matriz de Portfólio de Risco:

	Matriz de Portfólio de Risco				
Extremo					
Alto					
Médio					
Baixo					
Muito Baixo					
	Muito Baixo	Baixo	Médio	Alto	Extremo

Para mensuração dos conceitos para identificação e análise dos riscos os seguintes atributos foram utilizados:

Objetivo processo de Proteção à Privacidade: tratar dados pessoais assegurando a proteção à privacidade do titular, analisando o manuseio destas informações a partir da ocorrência dos seguintes eventos: mau uso do dado por membro interno, vazamento, captura ou intrusão de sistemas de armazenamento por membro externo.

Probabilidade - é a chance atribuída a ocorrência de evento que possam impactar na proteção à privacidade dos titulares de dados pessoais. Base - Artigo 50 § 2º:

> *Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados …...*

A mensuração da probabilidade de ocorrência destes eventos foi realizada tendo como parâmetro central o índice de volumetria ajustado pela escala supracitada (mau uso, vazamento, intrusão) operada pelo processo em exame. O cálculo da volumetria considerou como parâmetros para estabelecimento do valor da probabilidade:

Período de apuração do volume de dados pessoais tratados pelo processo - 12 meses

Índice de volumetria ajustada considera em um índice agregado os seguintes fatores: quantidade de titulares de dados x perfis de servidores com acesso aos dados, ponderados pela quantidade de manipulação mensal padrão destes dados (mau uso e vazamento) e pelo nível de interesse de intrusão para captura destes dados (intrusão) - 1- Baixo, dados públicos facilmente acessíveis; 2- Médio dados que podem possibilitar uso para cadastros ou divulgação externa; 3- Alto, dados que podem ser usados para fins de manipulação de comportamento,crédito ou sensíveis;

Faixas: mínima = 0; máxima >=ao máximo de dados

Tabela de classificação de probabilidade:

Índice de volumetria ajustado- Faixas	Classificação	Rótulo
0-900.000	1	Muito Baixo
900.001 - 1.800.000	2	Baixo
1.800.001 - 2.700.000,00	3	Médio
2.700.001 -3.599.999	4	Alto
>= 3.600.000	5	Extremo

Impacto é o resultado de um evento que impacta o atingimento do objetivo do processo em exame. O impacto foi estimado a partir da base legal para coleta do dado pessoal.

Base - Artigo 50 § 2º:

> *Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados …...*

Tabela de classificação de impacto:

Impacto na organização Fator base Legal LGPD	Classificação	Rótulo
Art. 7º, I - mediante fornecimento de consentimento pelo titular	3	Médio
Art 7º II - para o cumprimento de obrigação legal ou regulatória pelo controlador	2	Baixo
Art 7º 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;	1	Muito Baixo
Art. 7º 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;	2	Baixo
Art. 7º 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) ;	2	Baixo
Art. 7º VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;	2	Baixo
Art. 7º VIII -para a tutela da saude exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade	2	Baixo

sanitária;		
Art 7º 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	4	Alto
Art 7º X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.	1	Muito Baixo
Art. 11 I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;	5	Extremo
Art. 11 II, a - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para a) cumprimento de obrigação legal ou regulatória pelo controlador;	3	Médio
Art. 11 II, b - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;	3	Médio
Art. 11 II, c - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;	5	Extremo

Art. 11 II, d - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável parad) 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	2	Baixo
Art. 11 II, e - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para e) proteção da vida ou da incolumidade física do titular ou de terceiro;	2	Baixo
Art. 11 II, f - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para 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) Vigência	4	Médio
Art. 11 II, g - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para 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.	4	Médio
Não se aplica	1	Muito Baixo

Tabela de Correlação - Probabilidade x Impacto para Risco Inerente

Probabilidade	Impacto	Classificação Risco Inerente
1	1	Muito Baixo
2	1	Muito Baixo
3	1	Baixo
4	1	Médio
5	1	Alto
1	2	Muito Baixo
2	2	Baixo
3	2	Médio
4	2	Alto
5	2	Extremo
1	3	baixo
2	3	Médio
3	3	Alto
4	3	Alto
5	3	Extremo
1	4	Médio
2	4	Muito Baixo
3	4	Muito Baixo
4	4	Extremo
5	4	Extremo
1	5	Médio
2	5	Alto
3	5	extremo
4	5	extremo
5	5	extremo

Categorização da atividade de controle identificado para mitigar o risco inerente de vazamento, mau uso e intrusão - Níveis de segurança de ativos e sistemas

Não há medidas de segurança ou medidas ad hoc	1	Muito Baixo
Medidas reativas ou apenas políticas organizacionais não institucionalizadas	2	Baixo
Medidas reativas, organizacionais ou preventivas institucionalizadas	3	Médio
Medidas preventivas, reativas e políticas organizacionais institucionalizadas	4	Alto
Medidas preventivas, reativas e políticas organizacionais institucionalizadas e gerenciadas	5	Extremo

Tabela de Correlação para Risco Residual - Risco Inerente x Controles

Risco Inerente	Segurança de Ativos e Sistemas	Classificação Risco Residual
Muito Baixo	Muito Baixo	Muito Baixo
Baixo	Muito Baixo	Baixo
Baixo	Muito Baixo	Baixo
Médio	Muito Baixo	Médio
Alto	Muito Baixo	Alto
Muito Baixo	Baixo	Baixo
Baixo	Baixo	Baixo

Médio	Baixo	Médio
Alto	Baixo	Alto
Extremo	Baixo	Extremo
baixo	Médio	Médio
Médio	Médio	Médio
Alto	Médio	Alto
Alto	Médio	Alto
Extremo	Médio	Extremo
Médio	Alto	Muito Baixo
Muito Baixo	Alto	Muito Baixo
Muito Baixo	Alto	Muito Baixo
Extremo	Alto	Baixo
Extremo	Alto	Baixo
Médio	Extremo	Baixo
Alto	Extremo	Baixo
extremo	Extremo	Baixo
extremo	Extremo	Baixo
extremo	Extremo	Baixo
Baixo	Muito Baixo	Baixo
Muito Baixo	Muito Baixo	Muito Baixo
Extremo	Muito Baixo	Extremo
Muito Baixo	Muito Baixo	Muito Baixo
Muito Baixo	Médio	Médio

Apetite a Risco para o Processo: Aceitar sem tratamento os riscos configurados como Muito Baixos e Baixos

Respostas a Riscos para o Processo:
Aceitar - até o apetite definido
Mitigar - risco médio, alto e extremo
Mitigar/Compartilhar - risco potencializado por terceiros externos

Evitar - Não aplicável ao processo

Para mensuração das lacunas de procedimentos, governança e obrigações legais que possam impactar a ocorrência dos eventos de risco (mau uso, vazamento e intrusão) os seguintes atributos foram utilizados:

Gap Analysis - Lacunas de Procedimentos e Governança

Prazo indeterminado para guarda de dados pessoais sensíveis
Prazo indeterminado para guarda de dados pessoais em geral
Transferência de dados por aplicativos de mensagem ou e mail não institucionais
Utilização de planilhas pessoais para armazenamento e tratamento de dados pessoais sem proteção da organização
Documentos físicos armazenados sem proteção ou procedimento específico
Bases de dados pessoais sem proteção para manuseio, download, tratamento
Notificações de Privacidade -Transferência de dados pessoais para terceiros sem proteção direta ou regulação
Dados passados para atividades analíticas com acesso a outras áreas na organização

Tabela de Classificação de Criticidade - Lacunas de Procedimentos e Governança

Quantidade de Lacunas	Classificação de Risco
0-1	Muito Baixo

2-3	Baixo
4-5	Médio
6-7	Alto
8	Extremo

Gap Analysis - Lacunas de Obrigações Legais LGPD

Gestão de Consentimento -Consentimento sem condições e evidências do artigo 7º (quando compartilhados), 8º (demonstrar vontade do titular) e 9º (acesso facilitado ao tratamento)
Tratamento de DP como condição para fornecimento de produto ou exercício de direito sem destaque para este fato na coleta (§2º artigo 9º)
Base legal de legítimo interesse não cobre o disposto no artigo 10 - Transparência do tratamento do dado e não tem DPIA
Não mantém registro das operações de tratamento de dados pessoais que realizarem quando com base em Legítimo Interesse e ter DPIA (Descrição do tipo de dado, metodologia para coleta e para garantia da segurança da informação e mecanismos de mitigação de riscos) Art. 38
Falta de publicidade sobre a dispensa de consentimento quando dados sensíveis forem coletados nos termos do Artigo 11, II, a, b
Falta de consentimento para dados de menores
Não existe gestão do processo para proteção de direitos de titulares e procedimentos para solicitações e reclamações de privacidades (Art. 18)
Procedimentos e processos para confirmação de existência ou o acesso a DP mediante requisição do titular (Art. 19)
Existe tratamento de dados coletados com base no Ar. 4º III por terceiros privados

Não existe plano de respostas a incidentes e remediações (Art. 50)
Política e plano de treinamento de servidores para o processo (Art. 50)
Nomeação de servidores para responsabilidades do processo

Tabela de Classificação de Criticidade - Lacunas de Obrigações Legais LGPD

Quantidade de Lacunas	Classificação de Risco
0-2	Muito Baixo
3-5	Baixo
6-8	Médio
9-10	Alto
11-12	Extremo

Mapeamento do Ciclo de Vida dos Dados e Diagnóstico Inicial

O mapeamento do ciclo de vida dos dados e o resultado do diagnóstico inicial quanto a conformidade e riscos relacionado a proteção à privacidade no TJPB, consta do link:

https://docs.google.com/spreadsheets/d/1i0GfxL8slfDtw3hdUI8cK1zsEi8qdhBvr7bfi4HkCF4/edit?usp=sharing

Modelo de Relatório de Análise de Dados Pessoais (RAD)

A sistematização referencial para registro do mapeamento do ciclo de vida dos dados e do diagnóstico é apresentado no link a seguir.

https://docs.google.com/document/d/1RGyhOqVGGkvKdkkFWpNI99d_AY6eIuXLSv4HDlq6Jf8/edit?usp=sharing

Conteúdo do material audiovisual para capacitação de servidores e magistrados

A partir do contrato firmado com o Professor Cláudio Lucena, está em curso de desenvolvimento de material audiovisual para utilização no projeto inicial de sensibilização e capacitação de servidores e magistrados.

Os conteúdos deverão ser distribuídos em cronograma de capacitação do quadro de pessoal a ser definido no âmbito do Programa para ser suprido até o final do ano de 2020

Vídeo 1- Introdução à Proteção de Dados Pessoais

- Contexto
    - Privacidade e proteção de dados pessoais;
    - Por que o tema está na agenda;
    - Onde estamos no momento;
- Precedentes
    - Construção histórica no mundo;
        - privacidade;
        - legítima expectativa;
        - autodeterminação informativa;
        - controlador conjunto
    - A evolução do tema no Brasil;

- Quadro regulatório
    - conceito de dados pessoais
        - dados sensíveis
    - modelo europeu X modelo norte-americano;
    - anatomia de uma lei geral de proteção de dados pessoais

Temas a serem desenvolvidos nos demais vídeos;

- Direitos dos Titulares
- Bases legais para o processamento
- Responsabilidade dos agentes e regime de penalidades
- Auditoria de dados e registros de processamento
- Segurança da Informação: conceitos, ferramentas e boas práticas
- Segurança da Informação: Governança e Auditoria
- Revisão documental: contratos, termos de consentimento
- Avaliação de Impacto e Gestão de Riscos
- Framework de resposta a incidentes de segurança
- Agência Nacional e Conselho Nacional
- Transferência Internacional de Dados
- Atribuições e atuação do Encarregado
- Planejamento e implementação de conformidade

Proposta de estrutura para acompanhamento da maturidade

O Grupo de Trabalho propõe como estrutura básica para avaliação e acompanhamento da maturidade da LGPD no TJPB, sugere-se a que segue:

https://drive.google.com/file/d/1u2xG-2rEq08El153fOIqZoBztyh-o8Qm/view?usp=sharing

Check list inicial Projeto

ETAPA DO PROJETO DE CONFORMIDADE	ATIVIDADES JURÍDICAS	ATIVIDADES DE NEGÓCIOS	ATIVIDADES DA TI
Criação da Estrutura de Governança	Apoio na elaboração de políticas e documentos corporativos internos; Apoio consultivo para análise de normas setoriais à LGPD, específicas à cada segmento	Nomeação do Encarregado de Dados (DPO); Elaboração da Política de Privacidade e do Código de Ética/Conduta	Elaborar/Revisar Política de Segurança de Informação; Elaboração da Política de Privacidade
Gerenciamento de um Programa de Conscientização e Treinamento	Apoio na elaboração de materiais educativos para cliente interno e externo; Apoio no treinamento interno; Avaliar conteúdos informativos (quando aplicável)	Executar Capacitação de Novos Colaboradores; Garantir treinamento e capacitação dos Colaboradores envolvidos nas atividades que coletam dados privados; Requisitar evidências de conformidade dos prestadores de serviços e parceiros	Compartilhar conceitos de classificação de informação e divulgar critérios de controle de acesso; Conscientizar colaboradores sobre a Política de Segurança
Inventário de Dados Pessoais e Mecanismos de Transferência de Dados	Elaboração de contratos para proteger a privacidade na transferência de dados	Zelar pelo atendimento dos critérios de classificação e orientações das Políticas de Privacidade e de Segurança	Gerenciar bancos de dados e manter controles dos contratos que suportam procedimentos de transferências de dados privados
Gerenciamento de Riscos da Segurança de Informações	Gerenciar validades de contratos envolvendo processamento de dados e informações privadas	Atender aos requisitos das Políticas de Segurança e Privacidade	Manter Política de Segurança de Informação atualizada; Promover a conscientização dos colaboradores sobre a importância de cada item

Inclusão da Privacidade de Dados nas Operações	Promover análise, revisão e/ou elaboração de cláusulas contratuais específicas para proteção de informações privadas	Gerenciar a emissão dos termos de consentimento e manter controle sobre o prazo de validade de cada um	Disponibilizar mecanismos de controle de Segurança de Informação, adequados para proteção de privacidade em cada processo de negócio
Gerenciamento de Riscos de Terceiros	Análise, revisão e atualização dos contratos com prestadores de serviços e terceiros em geral	Acompanhar e manter atualizados os critérios de análise de riscos sobre fornecedores, prestadores de serviços, parceiros e terceiros em geral	Monitorar os fatores de risco dos prestadores de serviços relacionados à TI e SI
Gerenciamento de Alertas	N/A	Implementar avisos em pontos de coleta de informações, onde haja risco de exposição de dados pessoais durante o registro	Implementar avisos em sistemas ou aplicativos para coleta de informações, onde haja risco de exposição de dados pessoais durante o registro
Resposta a Solicitações e Reclamações de Terceiros	Atuação consultiva e orientações de conduta	Atendimento, Registro, Tratamento e Resposta aos pedidos de Titulares de Informações e/ou seus representantes legais	Disponibilizar mecanismos para registro, acompanhamento de atendimento (Protocolo) e autenticação de identidade do solicitante ou reclamante
Gerenciamento da Política Interna da Privacidade de Dados	Alinhamento das Políticas (Segurança de Informação/Privacidade) e Códigos (Ética/Conduta) para fim de proteção à privacidade	Oferecer subsídios aos Encarregados de Dados (DPO) para atualização dos itens da Política de Privacidade, adequando-a à realidade dos processos de negócios	Manter controles técnicos para suporte ao controle de acesso, classificação de informação e atualização da Política de Segurança de Informação, quando cabível

Programa de Gerenciamento na Perda de Dados	Suporte Jurídico no atendimento e resposta a incidentes envolvendo vazamentos de dados e informações	Elaborar e manter procedimentos de resposta e comunicação de vazamentos de dados, consoante diretrizes das Políticas de Segurança de Informação de Privacidade	Elaborar e manter Plano de Continuidade de Negócios atualizado e testado, envolvendo todas as áreas da organização
Práticas de Manuseio de Dados	Elaboração de cláusulas de privacidade específicas para suportar e proteger procedimento que envolvam manuseio de dados	Implementação de treinamento e programa de conscientização contínuos	Acompanhamento de prestadores de serviços que manuseiem banco de dados com informações privadas
Acompanhamento de Critérios Externos	Análise, recomendações de ajustes e atualizações de Políticas, quando cabível	Aplicação das recomendações e orientações das atualizações da Lei, nos procedimentos que envolvem dados privados	Atualização de processos e mecanismos de proteção técnica, quando cabível
Suporte e continuidade da estrutura de privacidade	Ação Consultiva, Manutenção de registros que demonstram a adoção das medidas para adequação das operações à LGPD	Implementação de processo de avaliação e acompanhamento de conformidade aos requisitos de privacidade da LGPD. Manutenção e atualização da Política de Privacidade	Manter Plano de Segurança de Informação atualizada; zelando pela educação continuada dos colaboradores, no seu conteúdo
Monitoramento de Novas Práticas Operacionais	Acompanhamento e suporte na elaboração de contratos que suportam novas práticas operacionais, envolvendo aspectos de privacidade de dados	Comunicação da criação de novos processos ou procedimentos que envolvam o tratamento de informações privadas, para atualização da documentação pertinente	Comunicação da criação de novos aplicativos ou sistemas, que envolvam o tratamento de informações privadas, para atualização da documentação pertinente