A JORNADA DO TJPB RUMO À IMPLEMENTAÇÃO DA LGPD

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A jornada do TJPB rumo à implementação daLGPD

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

Programa

Juiz Responsável: Dr. Jeremias de Cassio Carneiro de Melo

Equipe

Tecnologia da Informação:José Teixeira de Carvalho Neto
Encarregado de Proteção de Dados: Rodrigo Antonio Nóbrega
Área de Negócios: Eudes Moacir Toscano Júnior

Início : setembro 2020

Contato: cepd@tjpb.jus.br

ROTEIRO

Apresentação

O TJPB compartilha nesse documento o percurso seguido em seu projeto para implementação de Programa de Proteção de Dados e cumprimento dos requisitos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD).

Iniciado em janeiro de 2020, com a constituição de força tarefa de característica multidisciplinar, composta por representantes da área de negócios, jurídica e de tecnologia da informação, o projeto contou com amplo apoio da alta administração e o compromisso firme da equipe encarregada de seu desenvolvimento, sendo concluído em julho de 2020.

Como resultado do trabalho dessa força tarefa, foram definidos conceitos, critérios e metodologias para a realização do diagnóstico inicial da gestão de dados, a análise das lacunas de conformidade, a análise de risco dos processos e a definição de um plano de ação para adequação aos ditames legais e avanço nos níveis de maturidade de gestão. Adicionalmente foi apresentada uma proposta para constituição de um programa estruturante de proteção de dados no âmbito do TJPB, cuja implementação foi iniciada em agosto de 2020.

O roteiro de atividades e documentos produzidos pelo TJPB foram validados para uso interno pela alta administração, em sua versão inicial, e certamente contém lacunas e está sujeito a adequações ao longo do percurso.

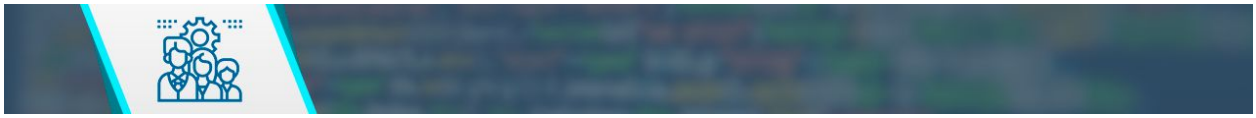
Compartilhamos o resultado do nosso projeto no intuito de inspirar e contribuir com outras entidades públicas no caminho a ser seguido rumo

a implementação efetiva dos requisitos da LGPD e na consequente proteção social dela decorrente.

1- Detalhamento do Projeto

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



1. Conscientização

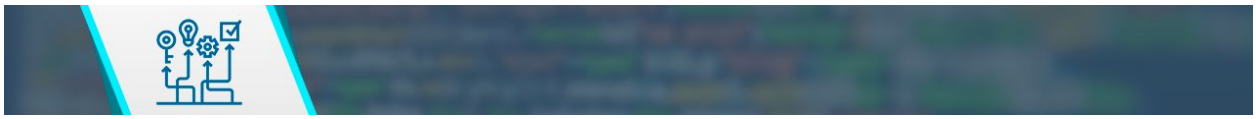
a. Levantamento de requisitos e necessidades;
b. Sensibilização e apoio da alta administração;
c. Definição do grupo de trabalho;
d. Conscientização e conhecimento sobre dados e parâmetros da LGPD –
   i. Estudos internos iniciais;
   ii. Capacitação da equipe do Projeto e áreas estratégicas

2. Projeto, Desenho e Metodologia

a. 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);
f. Definição de acompanhamento do projeto;

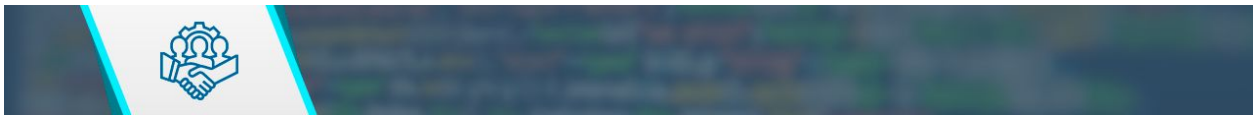


3. Mapeamento do Fluxo de Dados e Segurança da Informação

a. Levantamento e mapeamento com questionário e entrevistas, do ciclo de vida e do fluxo de dados;
b. Definição dos agentes de tratamento;
c. Levantamento, a partir do fluxo de dados de negócios, do inventário de ativos e avaliação de segurança da informação;
d. Identificação de estrutura de dados;

4. Documentação, Identificação e Análise de Riscos e Lacunas

a. Documentação - Relatório de de Análise de Dados (RAD);
b. Recomendação e validação das bases legais;
c. Classificação das lacunas de conformidade e de governança;
d. Classificação dos riscos dos processos;
e. Identificação de terceiros críticos por processo;

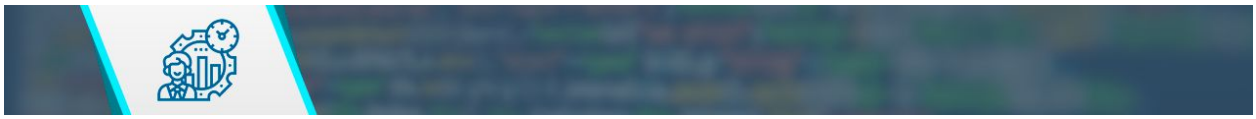


5. Governança de Proteção de Dados

a. Revisões e adequações contratuais;
b. Identificação e proposta de estrutura para acompanhamento da maturidade;
c. Elaboração de minuta de Política de Proteção de Dados;
d. Elaboração de material audiovisual para capacitação de servidores e magistrados;
e. Proposta de fases para Programa de Proteção de Dados;
f. Desenvolvimento de hotsite com informações sobre LGPD;

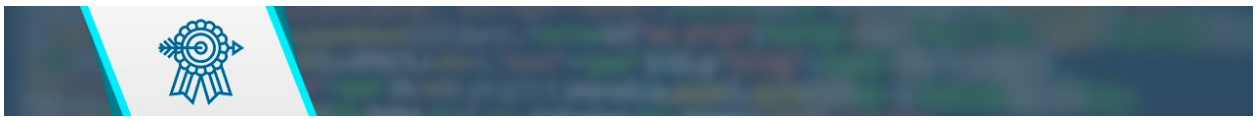
Fases para Programa de Proteção de Dados Pessoais e Privacidade - Proposta

Responsável: Alta Administração e Encarregado de Proteção de Dados
Objetivo: Orientar 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

1. 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*** –
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

2- Detalhamento Metodológicos e Registros

Definição de Áreas Estratégicas

As áreas e atividades estratégicas a serem abordadas e priorizadas pelo projeto 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, em cada atividade, quanto a utilização e proteção de dados pessoais e privacidade:

- sensibilidade;
- criticidade;
- abrangência da atividade;

Os parâmetros de avaliação seguiram a seguinte escala: 1- muito baixo a 5 muito alto e foram aplicados pela força tarefa em conjunto a partir de sua expertise com os processos envolvidos.

Atividades de Processamento Estratégicas - Escolha - **Modelo**

Área	**Atividade de Processamento**	SENSIBILIDADE	CRITICIDADE	ABRANGÊNCIA	TOTAL
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

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 e diagnóstico.

A seguir alguns exemplos, com caráter meramente ilustrativo, não refletindo a totalidade da modelagem utilizada pelo TJPB.

Dados Pessoais - Categorias
Nome
Data Nascimento
Filiação
RG

Titular de Dado
Servidor
Magistrado

Dados Sensíveis
Origem racial ou étnica
Convicção religiosa

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

Agentes Responsáveis pelo Tratamento
Controlador
Operador

Métodos de Transferências
E-mail institucional
E-mail não institucional

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;

Nível de Interesse na Intrusão
1 - Baixo, dados públicos facilmente acessíveis;

Parâmetros de prazo e forma para tratamento
Prazo indeterminado para guarda de dados pessoais sensíveis;
Prazo indeterminado para guarda de dados pessoais em geral;

Base Legal
Art. 7º, I - mediante fornecimento de consentimento pelo titular;
Art 7º II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

Compartilhamento dos dados
Outras entidades externas do Poder Público
Outras entidades externas privadas

Retenção de dados
Até 05 anos
Até 20 anos

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

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;

Modelagens Utilizadas

Coleta de Dados - Estrutura

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

https://docs.google.com/spreadsheets/d/1U1O836_1U_IGnGVP1jpRuJ2NxAkTVoxM8dw_i9nlf98/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.Para conhecer mais consultar :

https://pt.wikipedia.org/wiki/Diagrama_de_fluxo_de_dados

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

Para possibilitar o estabelecimento de políticas e salvaguardas, decorrentes de 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 e na ausência de metodologia padronizada por órgão regulador, o seguinte dicionário de risos foi definido:

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 foi estabelecida a clara definição do objetivo do processo e definidos os atributos para os parâmetros de probabilidade e impacto.

Para mensuração da probabilidade foi estabelecido o índice de volumetria ajustado. A métrica considera é formada por um índice agregado dos 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).

O impacto foi estimado a partir da base legal para coleta do dado pessoal.

Também foram definidas nessa fase: a tabela de correção para riscos inerentes; a categorização da atividade de controle identificado para mitigar o risco inerente, a partir dos níveis de segurança de ativos e sistemas; as tabelas de correlação para risco residual; definido o apetite a risco da organização e as respostas a riscos.

Para identificação e mensuração das lacunas de procedimentos, governança e obrigações legais que possam impactar a ocorrência dos eventos de risco foram definidos atributos específicos e definida a Tabela de Classificação de Criticidade

Relatório de Análise de Dados Pessoais (RAD) - Modelo

A sistematização referencial para registro do mapeamento do ciclo de vida dos dados e do diagnóstico é apresentado no link:
https://docs.google.com/document/d/1JFKZdcjsdjPCJjzaRCAwh39osRs30TWQrtCwirD1YBQ/edit?usp=sharing

Proposta de estrutura para acompanhamento da maturidade

O Grupo de Trabalho propõe que a estrutura para avaliação e acompanhamento da maturidade da LGPD no TJPB, seja desenvolvida na fase de programa, considerando, preferencialmente em conjunto, os seguintes sistemas:
The GDPR Maturity Framework
Avaliação de processo - ABNT NBR ISO/IEC 15504:2008
Information management maturity measurement tool (IM3)