Termo de Referência

ASSESSORIA E CONSULTORIA EM GOVERNANÇA DE PRIVACIDADE

Prefeitura do Município de

Itapecerica da Serra/SP

Prefeitura do Município de
Itapecerica da Serra

2023

(V 2.3)

Índice

1. RESUMO SITUACIONAL

1.1. A Prefeitura do Município de Itapecerica da Serra (PMIS - CONTRATANTE) é formada por Secretarias que, dentro de suas respectivas atribuições, são responsáveis por executar as diversas rotinas e entregar uma variedade de serviços aos munícipes de nossa cidade.

1.2. A abrangência deste projeto engloba as Secretarias da CONTRATANTE dispostas de acordo com a seguinte estrutura e suas respectivas áreas de atuação:

#	Unidade	Atuação	Quantidade de colaboradores
1	**Secretaria da Cultura**	- Coordenar, planejar, controlar e organizar as atividades culturais do Município; - Incentivar, difundir e desenvolver atividades culturais, festividades cívicas e comemorativas, certames e eventos artísticos, literários e vocacionais no Município; - Promover a administração e manutenção da Biblioteca Pública, bem como a guarda, controle, renovação e circulação do seu acervo; - Promover a coleta, guarda, conservação e preservação de documentos e demais peças que compõem a memória e o acervo artístico e histórico do Município.	60
2	**Secretaria da Habitação e Desenvolvimento Urbano**	Promover, coordenar, gerenciar e executar a Política Habitacional de Interesse Social, através da ação direta do Município ou através de convênios e programas com órgãos e entidades nacionais ou internacionais, buscando recursos que lhe permitam solucionar de maneira adequada a situação das moradias que ocuparam de forma inadequada áreas de preservação ambiental.	13
3	**Secretaria de Administração - Apoio Administrativo**	Dividida entre: Diretoria de Departamento, Divisão de Protocolo e Divisão de Manutenção do complexo Administrativo, funciona com um braço de apoio da Secretaria para a execução de atividades administrativas e de facilities.	29
4	**Secretaria de Administração - Departamento de Frota Municipal**	Acompanhamento e controle de conserto de veículos da frota municipal, peças, mão de obra, orçamentos, elaboração de documentos e relatórios mensais, controle de frequência de servidores, infrações de multas diárias quanto a identificação do condutor e desconto em folha de pagamento, controle de quantidade e distribuição de pães diários da prefeitura, parte diária dos veículos oficiais e alugados, notas fiscais e atestados, pronto-atendimento aos servidores quanto a férias, falta abonada, licença prêmio, atestados, acompanhamento médico, rotina administrativa do setor, disponibilização de requisições junto ao almoxarifado e suprimentos. Trata também da gestão da frota escolar do município.	88
5	**Secretaria de Administração - Gerência de Atendimento e Arquivo**	Reprodução de Documentos. Controla a qualidade e quantidade de reproduções; dá autenticidade às cópias reprográficas; organiza documentos e correspondências; registra termos de apensamentos e desapensamento; registra documentos no sistema; conserva e mantém documentos; controla entrada e saída de documentos; atende solicitações de documentos de todos os demais departamentos.	15

#	Unidade	Atuação	Quantidade de colaboradores
6	**Secretaria de Administração - Departamento de Recursos Humanos**	Realiza a gestão de RH da prefeitura, gerencia a divisão de protocolo, gerencia a Folha de Pagamento, elabora minutas de portarias, gerencia medicina ocupacional e todos os concursos públicos municipais	35
7	**Secretaria de Educação**	Gerenciar toda a educação municipal (processo de matrícula, gestão administrativa de escolas e gestão pedagógica) e suas 72 unidades escolares	1488
8	**Secretaria de Esportes e Lazer**	- Coordenar e desenvolver, nas diversas regiões do Município, a prática desportiva e de lazer aos munícipes; - Promover a inserção da sociedade, por meio da prática esportiva; - Promover a recreação em ruas e espaço de lazer; - Desenvolver a integração esportiva intermunicipal; - Realizar parcerias com as esferas estadual e federal, por meio de convênios; - Criar parcerias com instituições privadas, visando o encaminhamento de jovens que tenham condições de profissionalização; - Desenvolver, por meio do lazer, a sociabilização de crianças, jovens, adultos e membros da terceira idade; - Promover, por meio de eventos esportivos, o congraçamento e o intercâmbio dos diversos bairros do município.	84
9	**Secretaria de Finanças**	- Assistir e assessorar o Prefeito na elaboração de políticas, programas, planos, projetos, diretrizes e metas quanto aos aspectos financeiros do Município; - Supervisionar, coordenar e controlar os assuntos financeiros, fiscais, de lançamentos, arrecadação e fiscalização de tributos do Município, e demais receitas; - Supervisionar, coordenar e controlar o processamento das despesas, contabilização orçamentária, financeira, patrimonial e econômica; - Supervisionar, coordenar e controlar o recebimento, guarda e movimentação dos valores do Município; - Coordenar, controlar e manter atualizado o registro do cadastro mobiliário e imobiliário; - Elaborar Projeto de Lei de Diretrizes Orçamentárias, o Orçamento Anual, o Plano Plurianual, em conjunto com as demais Secretarias e em consonância com o disposto na Legislação Federal, Estadual e Municipal; - Promover a administração de material e patrimônio; - Centralizar, coordenar e supervisionar os serviços e assuntos relativos a padronização, aquisição, guarda, distribuição e controle de materiais e equipamentos; - Responsabilizar-se por tombamento, registro, inventário e proteção do patrimônio Municipal; - Responsabilizar-se pelas aquisições de materiais, contratações de obras e serviços, por meio de procedimentos licitatórios.	52
10	**Secretaria de Governo**	Responsável por gerenciar a TI do município, as políticas públicas e a ouvidoria	17

#	Unidade	Atuação	Quantidade de colaboradores
11	**Secretaria do Desenvolvimento Social e Relações do Trabalho**	- Coordenar e definir as diretrizes da Política Municipal da Assistência Social em parceria com o Conselho Municipal de Assistência Social; - Elaborar o Plano Municipal da Assistência Social em parceria com o Conselho Municipal de Assistência Social; - Organizar e gerir a rede municipal de inclusão e proteção social, os programas, projetos e serviços assistenciais; - Articular com outras políticas públicas a inclusão dos destinatários da Assistência Social; - Supervisionar, monitorar e avaliar as ações da Assistência Social no Município; - Estabelecer mecanismos de articulação com as outras esferas de Governo e com a Sociedade Civil para garantir apoio técnico e financeiro; - Desenvolver programas de qualificação de Recursos Humanos para a área de Assistência Social; - Coordenar o desenvolvimento de gestão pública de emprego e renda; - Articular parcerias entre Poder Público e entidades da Sociedade Civil com vistas à elaboração e execução de projetos da área de empregos e geração de renda; - Contribuir para a qualificação e requalificação profissional dos trabalhadores do Município; - Coordenar os serviços do Fundo Social de Solidariedade; - Manter relações organizacionais com a Vara da Infância e Juventude; - Gerir a execução de programas e projetos estaduais e federais em âmbito municipal.	133
12	**Secretaria de Obras**	- Coordenar e promover a construção dos prédios municipais; - Manter e controlar o uso de máquinas e equipamentos da Prefeitura; - Promover a construção, manutenção e conservação da rede viária do Município, de suas estradas e caminhos; - Executar e fiscalizar serviços de pavimentação asfáltica, guias e sarjetas e outras obras viárias; - Instruir e se manifestar em termos técnicos nas licitações para contratações de obras públicas; - Coordenar, analisar, orçar os custos, executar projetos de obras públicas e fiscalizá-las; - Gerenciar, fiscalizar e realizar acompanhamento técnico de convênios e das PREFEITURA DO MUNICÍPIO parcerias populares referentes às obras públicas; - Manter e controlar o uso da usina de asfalto e fábrica de artefatos de cimento; - Elaborar diretrizes visando captação de recursos para investimento por meio de convênios com outros órgãos, em todas as esferas de governo, que visem o desenvolvimento urbano do Município; - Apoiar a integração de programas e ações municipais, estaduais e federais referente à execução de projetos com utilização de recursos oriundos de convênios, contratos ou termos; - Gerir as ações e programas da Secretaria; - Participar da formulação de políticas das ações de saneamento básico.	20

#	Unidade	Atuação	Quantidade de colaboradores
13	**Secretaria de Planejamento e Meio Ambiente**	- Coordenar e executar a política, os planos, os projetos de obras e edificações e planejamento territorial do Município, aprovando-os ou não; - Planejar o uso e ocupação do solo no Município, especialmente em Zona Urbana; - Conceder, cassar ou recusar licenças, certidões e habite-se; - Estabelecer normas de edificação, de loteamento, arruamento a zoneamento a ordenação do território do Município; - Assessorar o processo de planejamento e Orçamento Municipal visando orientar, selecionar e integrar, com critérios compatíveis aos do Plano Diretor Estratégico, os programas e projetos a serem implementados pelo Poder Público ou com sua participação; - Promover e desenvolver estudos e projetos para implantação de áreas e empreendimentos urbanos de caráter inovador, que elevem o padrão funcional urbanístico e paisagístico do Município e atraiam novos investidores e usuários; - E gerenciar os demais aspectos do planejamento urbano municipal e do Meio Ambiente.	56
14	**Secretaria de Serviços Urbanos**	- Executar reparos na malha viária do Município; - Providenciar a limpeza das vias e logradouros públicos, a remoção do lixo e resíduos de qualquer natureza; - Promover e controlar os serviços de necrópoles; - Participar da formulação de política das ações de saneamento básico; - Coordenar e implementar, pelas Administrações Regionais do Valo Velho, Jardim Jacira e do Potuverá, os serviços e manutenções pertinentes à Secretaria Municipal de Serviços Urbanos; - Promover a manutenção e conservação das praças, parques, jardins e demais áreas públicas do Município.	188
15	**Secretaria de Trânsito**	- Coordenar os trabalhos da Guarda Municipal; - Assessorar o Prefeito em assuntos de segurança; - Coordenar e implementar as atividades de engenharia e a operação de tráfego, ordenando, planejando, organizando e disciplinando o uso do solo viário; - Coordenar, implementar, autorizar e delegar as atividades do serviço de transporte público, ordenando, planejando, organizando e disciplinando em regulamento próprio; - Credenciar agentes de fiscalização próprios ou de outros órgãos ou entidades que venham por força de convênios ou outros instrumentos executar isoladamente ou concomitantemente a fiscalização de trânsito e transportes; - Organizar e operar os sistemas do transporte coletivo e transporte de cargas como um todo, integrando-se aos sistemas de trânsito e transportes intermunicipais, de caráter regional, metropolitano, estadual ou federal; - Celebrar convênios, contratos e outros instrumentos legais com entes públicos ou privados, conforme art. 27, inciso V do Decreto Estadual nº 34.184, de 18 de novembro de 1991; - Exercer, dentro de seu limite territorial, todas as competências que lhe foram atribuídas pela Lei Federal nº 9.503, de 23 de setembro de 1997 (Código de Trânsito Brasileiro), e demais legislações e regulamentos, para o exercício do provimento, organização, gerenciamento e exploração do sistema de trânsito e transportes; - Conceder ou autorizar os serviços de táxis, veículos de aluguel e transporte coletivo.	45

#	Unidade	Atuação	Quantidade de colaboradores
16	**Secretaria de Turismo**	- Planejar ações que visem o desenvolvimento do turismo sustentável; - Promover eventos ligados ao esporte de aventura e ecoturismo; - Promover o relacionamento com as esferas de turismo intermunicipal, estadual e federal, para elaboração de convênios e parcerias, buscando a captação de recursos; - Garantir as atividades referentes ao Conselho Municipal de Turismo e definir suas diretrizes; - Participar de convenções, seminários e feiras referentes ao turismo, promovendo a divulgação das ações municipais; - Garantir participação efetiva na Câmara Técnica de Turismo, Lazer e Entretenimento do Subcomitê da Bacia Hidrográfica Cotia-Guarapiranga, assim como na Câmara de Turismo e Lazer no meio rural, do Estado de São Paulo; - Elaborar programas de qualidade turística em parceria com as demais Secretarias da Administração Municipal; - Garantir a divulgação dos atrativos turísticos municipais em meio de comunicação própria, bem como no Calendário Estadual de Eventos; - Fomentar ações que garantam a manutenção do Município na Classificação Nacional de Potencial Turístico; - Fomentar a realização de eventos tradicionais e datas comemorativas; - Promover estudos que visem o aproveitamento do potencial turístico do Município, buscando parcerias com órgãos públicos ou privados e instituições de ensino.	12
17	**Secretaria de Assuntos Jurídicos**	- Assessorar o Prefeito em todos os processos, atos, projetos de leis ou decretos e pareceres; - Manifestar-se nos processos judiciais nos prazos previstos em lei, bem como propor, contestar e acompanhar até final decisão as ações judiciais de interesse do Município e de qualquer órgão da Prefeitura; - Representar o Município em todos os tabelionatos, juízos e instâncias judiciais; - Examinar os aspectos jurídicos de atos administrativos e elaborar estudos de natureza jurídico administrativa; - Estabelecer processo administrativo e sindicância; - Coordenar, supervisionar e controlar os assuntos da dívida ativa do Município, promovendo sua cobrança amigável e judicial; - Redigir projetos de leis, decretos e outros atos que envolvam aspectos jurídicos, bem como promover a suplementação no âmbito do Município, da Legislação Federal e Estadual, no que couber; - Manifestar-se quanto aos aspectos jurídicos da utilização e alienação dos bens públicos e atuar nos casos de desapropriação; - Assessorar o Prefeito e os diversos órgãos da Prefeitura em assuntos jurídicos da Administração; - Promover a regularização de documentos de imóveis de propriedade da Prefeitura junto aos cartórios competentes, bem como coordenar a regularização fundiária no âmbito municipal; - Promover a elaboração de minutas de contratos, ajustes, escrituras e outros atos de natureza jurídica em que o Município for parte interessada; - Coordenar, controlar e implantar projeto de fiscalização no âmbito municipal para atender todas as áreas sujeitas a atuação do Poder Público.	50

1.3. A estrutura demonstrada acima é responsável por planejar, executar e gerenciar as principais rotinas operacionais da CONTRATANTE, que

podem ser divididas em *processos de negócio*, classificados quantitativamente e qualitativamente de acordo com a tabela a seguir:

Secretaria	Complexidade	Quantitativo
Secretaria da Cultura	Baixa	00
	Média	04
	Alta	00
	Subtotal	*04*
Secretaria da Habitação e Desenvolvimento Urbano	Baixa	05
	Média	05
	Alta	10
	Subtotal	*20*
Secretaria de Administração	Baixa	53
	Média	81
	Alta	298
	Subtotal	*432*
Secretaria de Educação	Baixa	50
	Média	190
	Alta	260
	Subtotal	*500*
Secretaria de Esportes e Lazer	Baixa	01
	Média	00
	Alta	00
	Subtotal	*01*
Secretaria de Finanças	Baixa	00
	Média	25
	Alta	154
	Subtotal	*179*
Secretaria de Governo	Baixa	05
	Média	05
	Alta	08
	Subtotal	*18*
Secretaria do Desenvolvimento Social e Relações do Trabalho	Baixa	00
	Média	07
	Alta	04
	Subtotal	*11*
Secretaria de Obras	Baixa	10
	Média	10
	Alta	20
	Subtotal	*40*
Secretaria de Planejamento e Meio Ambiente	Baixa	08
	Média	45
	Alta	06
	Subtotal	*59*
Secretaria de Serviços Urbanos	Baixa	30
	Média	10
	Alta	05
	Subtotal	*45*
Secretaria de Trânsito	Baixa	03
	Média	02
	Alta	01
	Subtotal	*06*
Secretaria de Turismo	Baixa	08
	Média	08
	Alta	00
	Subtotal	*16*
Secretaria de Assuntos Jurídicos	Baixa	10
	Média	10
	Alta	10
	Subtotal	*30*

Secretaria	Complexidade	Quantitativo
Total		1.361

1.3.1. Em termos comparativos, podemos considerar a classificação de complexidade de cada processo de negócio de acordo com a seguinte regra:

a) Baixa complexidade operacional:
   i. Possuem tarefas com grau baixo de dificuldade de execução
   ii. Possuem até 20 tarefas
   iii. Envolvem até duas unidades de negócio da CONTRATANTE (ou externas)
   iv. Não tratam dados pessoais sensíveis
   v. Não precisam atender a prazos legais ou judiciais
   vi. Não geram impactos financeiros, ao negócio ou imagem da organização se ocasionarem atrasos ou erros operacionais

b) Média complexidade operacional:
   i. Possuem tarefas com grau médio de dificuldade de execução
   ii. Possuem até 40 tarefas
   iii. Envolvem até três unidades de negócio da CONTRATANTE (ou externas)
   iv. Podem tratar dados pessoais sensíveis
   v. Podem precisar atender a prazo legais ou judiciais
   vi. Podem gerar impactos financeiros, ao negócio ou imagem da organização se ocasionarem atrasos ou erros operacionais

c) Alta complexidade operacional:
   i. Possuem tarefas com grau alto de dificuldade de execução
   ii. Possuem mais de 40 tarefas
   iii. Envolvem mais de três unidades de negócio da CONTRATANTE (ou externas)
   iv. Tratam dados pessoais sensíveis
   v. Precisam atender a prazo legais ou judiciais
   vi. Geram impactos financeiros, ao negócio ou imagem da organização se ocasionarem atrasos ou erros operacionais

1.4. Em termos de Tecnologia da Informação, a CONTRATANTE é atendida atualmente por um time interno, centralizado e composto por um total de 7 (sete) colaboradores que integram uma equipe da Secretaria de Administração. Esse atendimento é realizado de acordo com os seguintes parâmetros:

1.4.1. Atualmente não há um Plano Diretor de Tecnologia da Informação em uso pela equipe de TI do município;

1.4.2. Não há uma política de segurança da informação formal publicada e conhecida por todos;

1.4.3. As estações de trabalho (computadores dos colaboradores da CONTRATANTE) são protegidas pelo firewall do sistema operacional (Windows) e antivírus AVAST;

1.4.4. Os servidores de arquivos são LINUX e fazem uso do firewall IPTABLES;

1.4.5. Há internet em todas as estações de trabalho, com uso controlado e monitorado por relatórios de proxy (SARG);

1.4.6. As estações de trabalho têm suas portas USB liberadas para uso;

1.4.7. Todos os colaboradores possuem usuário e senha de rede individuais;

1.4.8. A TI possui um time de HelpDesk que executa atendimento de suporte a todas as secretarias. Esse time é dividido em 2 (dois) níveis de atendimento;

1.4.9. A rede interna da Prefeitura é do tipo estrela local, com autenticação na rede e compartilhamento de arquivos, atualmente sem a possibilidade de acesso remoto às estações de trabalho;

1.4.10. Os itens de configuração são gerenciados automaticamente por um sistema de inventário (OCS Linux) que abrange hardware e software;

1.4.11. Os backups são realizados diariamente no período noturno, e o armazenamento é externo;

1.4.12. A TI atende ao todo aproximadamente 1200 usuários, e todos possuem caixa de e-mail individual, hospedados em um fornecedor externo.

1.5. Os principais sistemas de gestão utilizados pela PMIS são:

1.5.1. Sistemas de gestão, suprimentos, Receita, Despesa, Patrimônio,

Dívida Ativa, IPTU, ISS, Tesouraria, Portal do cidadão, consulta licenças, holerites, férias, informe de rendimentos e Nota Fiscal eletrônica, todos fornecidos por terceiros na modalidade SaaS;

1.5.2. Sistema de gerenciamento de filas (TOTEN), sistemas de emissão de alvarás de taxi, idoso, cartão caminhão, transporte alternativo, transporte escolar, cadastramento anual do ensino infantil, cadastro de boletins – GCM, sistema de gestão bibliotecas municipais, todos desenvolvidos internamente;

1.5.3. Sistemas operacionais: Linux nos servidores e Windows nas estações de trabalho;

1.5.4. Bancos de Dados: Postgre, Dataflex e MySQL;

1.5.5. Linguagem de programação: PHP.

1.6. Desde 2018, com a promulgação da Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados (LGPD), a CONTRATANTE passou a analisar como deveria ser portar diante das novas definições legais e como isso afetaria suas rotinas operacionais, uma vez que é notório o grande volume de dados pessoais atualmente em tratamento pela CONTRATANTE para que seja possível cumprir suas obrigações administrativas.

1.7. Este projeto trata, portanto, da jornada de adequação da CONTRATANTE à Lei Geral de Proteção de Dados (LGPD), de acordo com os parâmetros aqui estabelecidos.

2. OBJETO

2.1. Trata-se de contratação de empresa para execução de serviços de consultoria e assessoria em Governança de Privacidade, contemplando os seguintes itens:

2.1.1. Diagnóstico da situação atual da Governança de Privacidade;

2.1.2. Reengenharia operacional para implementação de Programa de Governança de Privacidade;

2.1.3. Implantação de processos adicionais para Programa de Governança de Privacidade;

2.1.4. Treinamento e Capacitação sobre Governança de Privacidade;

2.1.5. Implantação de soluções tecnológicas de Governança de Privacidade.

3. JUSTIFICATIVA DO PROJETO

3.1. Com o advento da Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/18), cabe a Controladores garantir a privacidade de seus Titulares de Dados através da implementação de um Programa de Governança de Privacidade que implemente rotinas operacionais, tecnológicas e jurídicas que visem a proteção dos dados pessoais desses Titulares.

3.2. Em vigor desde setembro de 2020, a LGPD é uma legislação obrigatória e abrange também a operação de órgãos públicos, desde que esses órgãos realizem rotinas que façam uso de dados pessoais.

3.3. O Regulamento de Dosimetria e Aplicação de Sanções Administrativas, publicado pela ANPD[1] pavimentou o caminho para que, inclusive órgãos públicos, passassem a serem auditados e estarem bastante expostos a eventuais sanções, no caso de descumprimento.

3.4. Cabe ressaltar ainda que as sanções aplicadas pela ANPD não são as únicas maneiras da gestão pública ser impactada pelo descumprimento da LGPD. Além dos impactos iniciais que afetariam a privacidade dos Titulares de Dados, há a possibilidade desses Titulares de Dados acionarem o controlador na justiça, em busca de seus direitos.

3.5. Sendo assim, considerando a natureza operacional da PMIS, é fato que essa administração realiza muitas rotinas de tratamento de dados pessoais como controladores, e como operadores.

3.6. Logo, é de extrema importância que implementemos um programa de Governança de Privacidade com objetivo de nos adequarmos por completo aos requisitos da LGPD e, assim:

3.6.1. Garantir a privacidade dos titulares dos dados pessoais tratados por nós;

[1] https://www.gov.br/participamaisbrasil/regulamento-de-dosimetria-e-aplicacao-de-sancoes-administrativas

3.6.2. Evitar as sanções impostas pela Lei (sejam as aplicadas pela ANPD ou como reflexo de ações judiciais que já se acumulam pelo Brasil[2]).

3.7. O próprio Governo Federal já se manifestou demonstrando a importância de entes públicos se adequarem aos requisitos da LGPD e até mesmo publicou um guia que demonstra o escopo dessa adequação[3].

3.8. Não contamos, internamente, com colaboradores especializados em todos os temas e disciplinas operacionais, tecnológicas ou jurídicas que permeiam o escopo da LGPD, portanto, buscamos com esse projeto encontrar fornecedor externo que nos apoie nessa jornada.

4. DETALHAMENTO DO OBJETO

4.1. Diagnóstico da situação atual da Governança de Privacidade

4.1.1. O projeto se iniciará com uma avaliação da situação atual da CONTRATANTE em face aos requisitos estabelecidos na LGPD que direcionam para a implantação de um Programa de Governança de Privacidade.

4.1.2. Entendemos que essa avaliação deve ocorrer em todas as áreas listadas neste documento e considerando cada grupo de atividades operacionais em execução, intitulado "processo de negócio".

4.1.3. O diagnóstico é realizado mediante a execução das seguintes atividades que se complementam:

4.1.4. Modelagem BPMN AS-IS dos processos de negócio

a) A CONTRATADA deverá mapear as rotinas operacionais da CONTRATANTE e destacar nesse mapeamento os *ativos de informação*, *artefatos* e *dados pessoais* detectados em cada processo de negócio.

b) Esse mapeamento inclui:

i. Levantamento e entendimento do e fluxo das informações realizado em cada processo de negócio através da

[2] https://anppd.org/violacoes
[3] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

realização de entrevistas com os colaboradores da CONTRATANTE;

ii. Modelagem desse fluxo em diagramas BPMN;

iii. Aprovação da modelagem com os colaboradores da CONTRATANTE que serviram de fonte de informação.

c) Produtos de trabalho a serem entregues:

i. Diagramas BPMN 2.0 dos processos de negócio da CONTRATANTE em formato eletrônico (HTML e qualquer formato editável);

ii. Inventário dos objetivos institucionais de cada processo de negócio;

iii. Inventário dos processos disponibilizados em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.1.5. Inventário dos Dados Pessoais

a) A CONTRATADA deverá levantar, inventariar e classificar os *metadados pessoais* em uso pela CONTRATANTE em cada processo de negócio modelado tal como definido anteriormente;

b) A CONTRATADA deverá levantar informações referentes a todo o ciclo de vida de cada dado pessoal encontrado, abrangendo: coleta, processamento, compartilhamento e exclusão (quando houver).

c) Os metadados devem ser classificados em compatibilidade com a LGPD e com o Decreto Federal nº 10.046/19;

d) Deve-se associar cada metadado encontrado com seus respectivos documentos (artefatos), ativos de informação (físicos ou eletrônicos) e processos de negócio.

e) Produtos de trabalho a serem entregues:

i. Inventário dos metadados, ativos e artefatos associados disponibilizados em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.1.6. Mapeamento dos tratamentos de dados pessoais e suas respectivas bases legais

a) Todo dado pessoal inventariado em qualquer processo de negócio é utilizado para um ou mais fins;

b) O uso desses dados endereça um tratamento de dado pessoal específico, que, por sua vez, deve ser justificado (ou sustentado) por uma determinada base legal;

c) A LGPD traz em seus artigos 7º e 11º as hipóteses de tratamento de dados pessoal que podem justificar cada um desses tratamentos, e caberá à CONTRATADA identificar esses tratamentos, inventariá-los e associá-los à suas hipóteses da LGPD e a eventuais fundamentos legais adicionais que permitem, legalmente, a realização do tratamento.

d) Produtos de trabalho a serem entregues

i. Inventário dos tratamentos de dados realizados pela CONTRATANTE em cada um de seus processos de negócio e suas respectivas hipóteses da LGPD e eventuais fundamentos legais externos, disponibilizados em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.1.7. Análise de Medidas Administrativas de Privacidade e Segurança de Dados

a) Caberá à CONTRATADA analisar todas as medidas administrativas atualmente em uso que enderecem regras sobre os temas "privacidade" e/ou "segurança da informação", sejam elas implícitas ou explícitas.

b) Essas medidas estão separadas em políticas e cláusulas contratuais com fornecedores, e precisam ser avaliadas quanto a:

i. Nível de exequibilidade da medida;

ii. Responsável pela manutenção da medida;

iii. Escopo da medida em face aos requisitos da LGPD.

c) Produtos de trabalho a serem entregues:

i. Inventário das medidas administrativas atualmente em uso pela CONTRATANTE e análise de seus parâmetros,

disponibilizadas em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.1.8. Análise de Medidas Técnicas de Privacidade e Segurança de Dados

a) Caberá à CONTRATADA inventariar e avaliar todas as medidas técnicas de segurança já implementadas nas rotinas de tratamento de dados pessoais em uso pela CONTRATANTE em face aos parâmetros da LGPD.

b) As medidas técnicas são implementadas em cada ativo de informação utilizado na execução dos diversos tratamentos de dados realizados pela CONTRATANTE.

c) A análise dessas medidas técnicas resultará na análise do nível de confiabilidade de cada ativo, que é composto pelos aspectos de Confidencialidade, Integridade e Disponibilidade da informação desse ativo.

d) Produtos de trabalho a serem entregues:

i. Inventário das medidas técnicas de segurança atualmente implementadas em cada ativo em uso pela CONTRATANTE disponibilizadas em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência);

ii. Análise do nível de confiabilidade de cada ativo de informação utilizado pela CONTRATANTE de acordo com os parâmetros definidos na norma ISO/IEC 27.001 disponibilizada em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.1.9. Análise de riscos de Privacidade e Segurança da Informação

a) Após todos os inventários e análises realizadas anteriormente e descritas acima nas demais atividades a serem executadas pela CONTRATADA, será possível se realizar uma análise completa de todos os riscos que a CONTRATANTE atualmente enfrenta em relação aos aspectos de privacidade e segurança da informação de acordo com a LGPD.

b) Caberá então à CONTRATADA realizar essa análise de riscos composta por:

i. Levantamento, inventário e análise de cada risco de Privacidade e Segurança da Informação verificado na CONTRATANTE em face aos requisitos da LGPD com base nas informações previamente obtidas no projeto;

ii. Elaboração de estratégias de enfrentamento desses riscos de acordo com seu impacto e probabilidade de acionamento;

iii. Elaboração de Relatório de impacto de privacidade com base nas informações obtidas em concordância com o inciso XVII do Art. 5º e Art. 38 da LGPD.

c) Produtos de trabalho a serem entregues:

i. Inventário de todos os Riscos de Privacidade e Segurança da Informação atuais da CONTRATANTE disponibilizado em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência);

ii. Emissão do Relatório de Impacto de Privacidade (DPIA) pré-adequação, disponibilizado em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.1.10. Elaboração de Plano de Ação para implementação de programa de Governança de Privacidade

a) Após terminada todas as análises da situação atual da CONTRATANTE no que diz respeito à Governança de Privacidade, caberá à CONTRATADA definir todas as mudanças que serão ser realizadas para garantir a adequação operacional, tecnológica e jurídica do órgão à LGPD.

b) Essas mudanças deverão constar em um documento formal intitulado "Plano de Ação", onde a CONTRATADA deverá definir todos os parâmetros a serem modificados ou implementados na sequência do projeto para garantir completa adequação da CONTRATANTE à LGPD.

c) Nesse documento deverão constar as seguintes informações:

i. Procedimentos e rotinas de tratamento de Dados Pessoais que precisarão ser alterados e quais alterações deverão ser realizadas;

ii. Medidas administrativas de segurança e que precisarão ser alteradas ou implementadas (políticas e cláusulas contratuais);

iii. Especificações das medidas técnicas de segurança que precisarão ser alteradas ou implementadas por conta da CONTRATANTE;

iv. Novos processos de negócio que deverão ser implementados;

v. Ferramentas que deverão ser implementadas pela CONTRATADA ou pela CONTRATANTE para apoiar as mudanças previstas;

vi. Treinamentos e capacitações que deverão ocorrer na equipe da CONTRATANTE.

d) Produtos de trabalho a serem entregues:

i. Documento formal do Plano de Ação disponibilizado em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.2. Reengenharia operacional para implementação de Programa de Governança de Privacidade

4.2.1. Trata-se da realização de serviços que colocarão em prática o Plano de Ação definido anteriormente neste Termo de Referência.

4.2.2. A reengenharia é alcançada pela execução das seguintes atividades que se complementam:

4.2.3. Modelagem BPMN TO-BE dos processos de negócio

a) A CONTRATADA deverá modelar os novos fluxos operacionais da CONTRATANTE e destacar nesse mapeamento os *ativos de informação*, *artefatos* e *dados pessoais* utilizados em cada processo de negócio.

b) Essa atividade inclui:

i. Modelagem desse fluxo em diagramas BPMN;

ii. Aprovação da modelagem com os colaboradores da CONTRATANTE que irão executar os novos fluxos.

c) Produtos de trabalho a serem entregues:

i. Diagramas BPMN 2.0 dos novos processos de negócio da CONTRATANTE em formato eletrônico (HTML e qualquer formato editável);

ii. Inventário dos objetivos institucionais de cada processo de negócio;

iii. Atualização do inventário dos processos disponibilizados em ferramenta de Governança (ver tópico 4.5 deste Termo de Referência).

4.2.4. Implantação dos Processos de Negócio TO-BE

a) Após definição e aprovação da nova versão dos processos de negócio da CONTRATANTE agora adequados à LGPD, caberá à CONTRATADA suportar a operação dessa nova realidade operacional, dando segurança à CONTRATANTE na execução das novas rotinas.

b) Caso as mudanças operacionais endereçarem modificações em qualquer ativo de informação da CONTRATANTE, será responsabilidade da CONTRATANTE prover essas modificações e caberá à CONTRATADA dar suporte e acompanhar essas modificações, garantindo compatibilidade das necessidades em relação às modificações tratadas pela CONTRATANTE.

c) As atividades de implantação da nova realidade operacional da CONTRATANTE incluem os seguintes serviços a serem realizados pela CONTRATADA:

i. Elaboração de templates (modelos) necessários para a execução da nova versão dos processos;

ii. Elaboração de especificações funcionais para eventuais modificações em ativos de informação que deverão ser realizadas pela CONTRATANTE;

iii. Acompanhamento das alterações tecnológicas implementadas pela CONTRATANTE para atendimento à nova versão dos processos;

iv. Acompanhamento das rotinas operacionais da nova versão dos processos para suporte operacional.

d) Essas atividades devem ser realizadas em compatibilidade com as capacitações realizadas pelo projeto (ver tópico 4.4 deste Termo de Referência).

e) Produtos de trabalho a serem entregues:

i. Templates (modelos) de novos artefatos a serem utilizados pela CONTRATANTE;

ii. Especificações funcionais com definições de modificações a serem realizadas nos ativos de informação;

iii. Relatório de acompanhamento de implantação de novas versão de processos de negócio.

4.2.5. Elaboração das novas Medidas Administrativas de Privacidade e Segurança de Dados

a) A CONTRATADA deverá elaborar as políticas de privacidade, de segurança da informação e as cláusulas contratuais padrão que tratem dos temas "privacidade" e "segurança da informação" para contratos com colaboradores e fornecedores da CONTRATANTE, de acordo com os parâmetros estabelecidos pela LGPD.

b) Caberá também à CONTRATADA apoiar o processo de publicação e aprovação das Medidas Administrativas de Privacidade e Segurança de Dados para ciência e aceite a cada público específico para cada um dos documentos.

c) Produtos de trabalho a serem entregues:

i. Política de privacidade compatível com a LGPD;

ii. Política de segurança de dados compatível com a LGPD;

iii. Modelos de contratos com cláusulas-padrão de privacidade e segurança de dados.

4.2.6. *Acompanhamento implementação e ajustes das Medidas Técnicas de Privacidade e Segurança de Dados*

a) Caberá à CONTRATANTE realizar as melhorias em sistemas de segurança lógicos e físicos para atender a LGPD, visando aumentar o nível de confiabilidade dos ativos de informação, de acordo com as análises e riscos apontados pelo projeto.

b) Caberá à CONTRATADA apoiar e prestar consultoria à CONTRATANTE durante a implementação dessas melhorias.

c) Durante a execução da aquisição e/ou implantação de soluções tecnológicas que irão melhoras as Medidas Técnicas de Segurança de Dados, a CONTRATADA deverá disponibilizar colaboradores especializados nos temas para guiar a CONTRATANTE nas ações e validar as implementações.

d) Produtos de trabalho a serem entregues:

i. Relatórios de acompanhamento de atividades de aquisição e/ou implementação de Medidas Técnicas de Segurança de Dados.

4.3. Implantação de processos adicionais para Programa de Governança de Privacidade

4.3.1. O Plano de Ação listará os ajustes operacionais a serem realizados na CONTRATANTE para completa implementação do Programa de Governança de Privacidade e esses ajustes hora endereçarão modificações nos processos de negócio do órgão (ver tópico 4.2), hora endereçarão a necessidade de se implantar novas rotinas operacionais, frutos dos controles estabelecidos pela LGPD.

4.3.2. Caberá à CONTRATADA implementar na CONTRATANTE os seguintes processos de negócio:

a) Gestão de Direitos dos Titulares de Dados, conforme Artigos 17 a 22 da LGPD;

b) Gestão de Incidentes e Notificações de violação de Dados Pessoais, conforme Art. 48 da LGPD;

c) Gestão de Consentimento, conforme especificações da LGPD, em especial o Art. 8° dela;

d) Análise de Risco e Impacto de Privacidade, conforme especificações da LGPD, em especial o Art. 38 da Lei.

4.3.3. Essa implementação inclui a realização das seguintes atividades por parte da CONTRATADA:

a) Documentar as regras desses processos de negócio modelando as atividades e sequência dos fluxos de ponta-a-ponta;

b) Aprovar os processos com os líderes operacionais da CONTRATANTE e suportar a operação dessa nova realidade operacional;

c) Caso um processo enderece modificações em qualquer ativo de informação da CONTRATANTE ou integração técnica entre a solução de gestão do processo e os sistemas legados da CONTRATANTE, será responsabilidade da CONTRATANTE prover essas modificações e caberá à CONTRATADA dar suporte e acompanhar essas modificações, garantindo compatibilidade das necessidades em relação às modificações tratadas pela CONTRATANTE;

d) Essas atividades devem ser realizadas em compatibilidade com as capacitações associadas aos novos Processos de Negócio da LGPD implementados (tópico 4.4 deste Termo de Referência);

e) Produtos de trabalho a serem entregues:

i. Diagramas BPMN 2.0 dos processos em formato eletrônico (HTML e qualquer formato editável;

ii. Templates (modelos) de novos artefatos a serem utilizados pela CONTRATANTE na execução do novo processo;

iii. Relatório de acompanhamento de implantação do novo processo;

iv. Disponibilização das ferramentas que permitirão a execução dos novos processos (tópico 4.5 deste Termo de Referência.

4.4. Treinamento e Capacitação sobre Governança de Privacidade

4.4.1. Espera-se que o time da CONTRANTE adquira, ao longo da execução do projeto, fluência nas disciplinas, termos e técnicas envoltas na implantação de programa de Governança de Privacidade.

4.4.2. Dessa forma, planeja-se a execução de diversos treinamentos e workshops que permitam a transferência de conhecimento e tecnologia entre as partes.

4.4.3. Esses treinamentos e rodadas de capacitação devem ser planejados durante a execução do projeto, de forma a maximizar os resultados de absorção dos conhecimentos associados a cada um deles.

4.4.4. Os seguintes tópicos deverão ser tratados durante a realização dos serviços de treinamento e capacitação sobre Governança de Privacidade:

4.4.5. Conhecimentos básicos sobre a Lei Geral de Proteção de Dados (LGPD)

a) Ementa mínima:
   i. Como surgiu a Lei Geral de Proteção de Dados;
   ii. Os principais aspectos e temas tratados pela LGPD;
   iii. Como a LGPD se aplica no setor público;
   iv. Quais os passos para se completar a adequação à LGPD.

b) Público-alvo: Líderes operacionais da CONTRATANTE;

c) Quantidade de treinamentos planejados: 2 (dois).

4.4.6. Aspectos tratados na reengenharia dos processos (TO-BE)

a) Ementa mínima:
   i. Todas as modificações definidas, acompanhadas de suas justificativas;
   ii. Modificações tecnológicas realizadas pela CONTRATADA e as que são de responsabilidade da CONTRATANTE para suportar a execução dos processos atualizados.

b) Público-alvo: Líderes operacionais da CONTRATANTE;

c) Quantidade de treinamentos planejados: 1 (um) para cada processo ou área de negócio.

4.4.7. *Aspectos dos novos processos de negócio previstos na LGPD*

a) Ementa mínima:

i. Gestão de Direitos dos Titulares de Dados, conforme Artigos 17 a 22 da LGPD;

ii. Gestão de Incidentes e Notificações de violação de Dados Pessoais, conforme Art. 48 da LGPD;

iii. Gestão de Consentimento, conforme especificações da LGPD, em especial o Art. 8° dela;

iv. Análise de Risco e Impacto de Privacidade, conforme especificações da LGPD, em especial o Art. 38 da Lei;

v. Como utilizar as ferramentas disponibilizadas pelo projeto para a execução dos processos aqui listados.

b) Público-alvo: Líderes operacionais da CONTRATANTE;

c) Quantidade de treinamentos planejados: 1 (um) para cada processo listado na ementa.

4.4.8. *Preparação do Encarregado de Proteção de Dados (DPO)*

a) Ementa mínima:

i. Fundamentos de segurança da informação de acordo com a norma ISO/IEC 27.001;

ii. Papéis e responsabilidades do Encarregado de Proteção de Dados (DPO) de acordo com a LGPD;

iii. Como gerenciar um Sistema de Gestão de Privacidade e Proteção de Dados (SGPD) em conformidade com a LGPD utilizando as ferramentas disponibilizadas pelo projeto.

b) Público-alvo: O Encarregado de Proteção de Dados (DPO) da CONTRATANTE e sua equipe;

c) Quantidade de treinamentos planejados: 1 (um) treinamento para cada um dos tópicos listados na ementa.

4.4.9. A execução dos treinamentos deve ocorrer de acordo com as seguintes premissas:

a) Planejamento do treinamento, incluindo os dados sobre o instrutor que deve possuir competências técnicas suficientes para ministrar as aulas, e a quantidade de horas estimadas

para execução de cada treinamento que seja suficiente para cumprir os objetivos de cada capacitação;

b) Elaboração de apostila digital com conteúdo do treinamento;

c) Execução da capacitação nos temas definidos de forma remota;

d) Elaboração de relatório de resultado do treinamento.

e) Produtos de trabalho a serem entregues:

i. Plano de treinamento;

ii. Apostila digital com o conteúdo do treinamento;

iii. Relatório de resultado do treinamento.

4.5. Implantação de soluções tecnológicas de Governança de Privacidade

4.5.1. Buscando garantir a sustentabilidade operacional do projeto e maximizar os resultados obtidos pelo sucesso esperado do projeto, define-se que todas as atividades de implementação do programa de Governança de Privacidade, bem como os inventários de entidades realizados durante a prestação de serviços deverão ser entregues pela CONTRATADA em uma solução de governança completa, disponibilizada para esse específico fim.

4.5.2. Essa solução deve possuir ferramentas, módulos e funcionalidades que, integradas e em conjunto, atendam ao seguinte escopo:

4.5.3. Requisitos gerais:

a) Ser fornecida modalidade Software as a Service – SaaS e disponibilizada via web;

b) Ser acionada tanto via browser como um aplicativo mobile em dispositivos iOS e Android;

c) Estar hospedada em um ambiente de nuvem seguro, que possua padrões de qualidade comprovados nos quesitos de *segurança da informação*, *gerenciamento de serviço de TI* e *privacidade*;

d) Ter um acordo de nível de serviço que garanta disponibilidade de, no mínimo, 98%;

e) Possuir fluxos de aprovação automatizados customizáveis, sem a necessidade de codificação;

f) Possuir a capacidade de ser customizada em ambiente amigável, sem a necessidade de codificação;

g) Se integrada, nativamente, a ferramentas de produtividade como o pacote Office (Word e Excel);

h) Possuir a capacidade de exportar e importar dados através de planilhas em formato .XLSX sem a necessidade de codificação adicional;

i) Se integrada, nativamente, a soluções de envio de e-mails.

4.5.4. Requisitos específicos:

a) Permitir o inventário e gestão das informações de adequação à LGPD, a partir do:

i. Cadastro de pessoas envolvidas no projeto incluindo nome, e-mail e foto;

ii. Cadastro de etapas de adequação à LGPD distintas com indicativo de uma pessoa responsável pela etapa (previamente cadastrada), data de início e fim da etapa e indicativo se a etapa está em andamento;

iii. Cadastro de áreas de negócio (órgãos/unidades);

iv. Cadastro de processos de negócio, com possibilidade de cadastro de modelagem BPMN navegável gráfica (em formato .HTML) para cada processo e associação do processo com cada área de negócio da CONTRATANTE;

v. Fluxo automatizado de aprovação do processo cadastrado por e-mail;

vi. Cadastro de ativos da informação utilizados em processos previamente cadastrados, com diferenciação para ativos eletrônicos e físicos;

vii. Cadastro de análise de confiabilidade da informação de cada ativo da informação, permitindo cadastro independente de características de Confidencialidade, Integridade e Disponibilidade das informações tratadas pelo ativo e possibilidade de categorização automática do nível de confiabilidade do ativo de acordo com a classificação de cada item da CID de informação do ativo;

viii. Cadastro de medidas técnicas associadas a cada ativo da informação previamente cadastrado, com classificação se a medida técnica é de segurança ou prevenção;

ix. Cadastro de artefatos tratados por cada ativo da informação cadastrado, com diferenciação do tipo de titular de dados que tem seus dados pessoais tratados no Ativo (munícipe, fornecedor/operador, colaborador do controlador);

x. Cadastro de metadado pessoal, tratado em cada artefato previamente cadastrado e possibilidade de classificação do metadado pessoal compatível com o Decreto Federal nº 10.046/19;

xi. Associação entre metadado pessoal, artefato, ativo e processo de negócio cadastrado, permitindo a gestão da dependência entre esses itens e a análise de impacto no gerenciamento de configuração da informação;

xii. Cadastro de tratamentos de dados pessoais com possibilidade de indicação da base lega/hipótese de tratamento da LGPD (Arts. 7º e 11º da LGPD) associada e possibilidade de indicação de fundamentação legal associada à finalidade (Lei ou Decreto) e associação com processos de negócio;

xiii. Possibilidade de se associar um artefato e seus metadados pessoais a cada tratamento de dados pessoais, com indicação se essa associação atende ou não ao princípio da Necessidade do tratamento de Dados (inciso III do Art. 6º da LGPD);

xiv. Cadastro de fundamento legal (Lei ou Decreto) para associação com o tratamento de dados pessoais;

xv. Cadastro de medidas administrativas de segurança (políticas) com possibilidade de se anexar documentos e realizar uma análise qualitativa automática dos principais parâmetros de cada medida administrativa cadastrada;

xvi. Cadastro de contratos com titulares e operadores com possibilidade de se anexar documentos e realizar uma

análise qualitativa automática dos principais parâmetros de cada contrato cadastrado;

xvii. Associação de tratamentos de dados pessoais que indiquem o uso de Operadores com contratos de operadores, indicando quais finalidades são cobertas por quais contratos;

xviii. Cadastro e gestão de riscos e impactos de privacidade e proteção de dados, com possibilidade de associação de cada risco a processos de negócio, ativos e tratamento de dados previamente cadastrados e definição de uma pessoa responsável por tratar o risco;

xix. Possibilidade de definição da criticidade do risco a partir do cruzamento de informações entre o impacto e a probabilidade de cada risco;

xx. Fluxo automatizado de aviso para tratamento de riscos cadastrados/disparados;

xxi. Cadastro de atividades de adequação incluindo data de início/fim, pessoa responsável pela atividade, status e etapa associada;

xxii. Fluxo automatizado de aviso para atividades de adequação cadastradas/encerradas.

b) Possuir módulo para gestão de Direito dos Titulares de Dados, contendo as seguintes funcionalidades:

i. Para uso de Titulares de Dados:

- Acesso externo (web, via portal HTML a ser publicado no website da CONTRATANTE) a Titulares de Dados para solicitação de informações ao Encarregado de Proteção de Dados da CONTRATANTE sobre a LGPD, sem limite de usuários;
- Cadastro com validação de autenticidade do Titular através do uso de fotos de rosto e fotos de documentos);
- Cadastro de nova solicitação ao controlador, dividida por tipo de solicitação;

- Consulta de solicitações anteriores e seus status e tratativas;
- Recebimento de e-mail automático quando houve resposta a cada uma de suas solicitações.

ii. Para uso do Encarregado de Proteção de Dados (DPO):

- Acesso via browser e aplicativo móvel;
- Aprovação de cadastros de Titulares de Dados;
- Cadastro de tipos de solicitações de Titular de Dados com definição de SLA máximo para cada tipo de solicitação;
- Recebimento de solicitações criadas no Portal web para uso do Titular de Dados;
- Recebimento de alertas para novas solicitações e proximidade de expiração de SLA de solicitações;
- Possibilidade de responder, em campo texto e com anexo de documentos adicionais, as solicitações dos Titulares de Dados;
- Possibilidade de encerramento de solicitações (controle de status).

c) Possuir módulo para Gestão de Incidentes e Notificações, contendo as seguintes funcionalidades:

i. Cadastro de Incidentes de segurança com possibilidade de se associar riscos e ativos previamente cadastrados a cada incidente;

ii. Possibilidade de indicação se o incidente inclui ou não violação de dados pessoais;

iii. Possibilidade de se anexar documentos externos ao incidente;

iv. Possibilidade de se indicar uma pessoa responsável previamente cadastrada como responsável pelo incidente;

v. Cadastro de uma Notificação a partir de um Incidente previamente cadastrado;

vi. Possibilidade de se anexar documentos externos à notificação;

vii. Possibilidade de se indicar uma pessoa responsável previamente cadastrada como responsável pela notificação;

viii. Possibilidade de se indicar se a notificação tem como objetivo informar a ANPD, Titulares de Dados ou ambos;

ix. Possibilidade de se indicar uma lista de Titulares de Dados (e-mails) a serem notificados quando a notificação tiver como objetivo informá-los;

x. Possibilidade de se indicar, manualmente, tratamentos de dados e ativo da informação associados à notificação;

xi. Possibilidade de indicação de justificativa no caso de demora para geração da notificação;

xii. Possibilidade de indicação da natureza dos dados pessoais envolvidos, Titulares de Dados envolvidos e medidas tomadas para mitigar os efeitos do incidente associado à notificação;

xiii. Geração automática do documento de notificação (em formato .pdf) para ANPD/Titulares de Dados de acordo com os requisitos da LGPD, incluindo, no mínimo, as informações definidas pela ANPD;

xiv. Envio de e-mail do documento final da notificação a Titulares de Dados, com controle de data de envio e guarda da cópia das notificações enviadas.

d) Possuir módulo de Gestão de Consentimento, contendo as seguintes funcionalidades:

i. Geração de Termo de Consentimento via e-mail;

ii. Possibilidade de se selecionar tratamento de dados pessoais, previamente cadastrado, que utiliza como hipótese de tratamento/base legal o consentimento do Titular;

iii. Possibilidade de se informar uma lista de e-mails dos titulares que irão receber o pedido de consentimento (individual ou em lote);

iv. Possibilidade de se indicar um prazo máximo do consentimento;

v. Criação automática do Termo de Consentimento contendo as seguintes informações:
   - Processo de negócio envolvido no consentimento (associado ao tratamento de dado pessoal selecionado);
   - Tratamento de dados pessoais associados ao consentimento;
   - Indicação se o tratamento realiza o compartilhamento dos dados com terceiros;
   - Indicação dos detalhes do compartilhamento dos dados com terceiros, se esse for o caso;
   - Lista de metadados pessoais associados ao tratamento selecionado;
   - Link para a política de privacidade do controlador;
   - Prazo de validade do consentimento;
   - Detalhes sobre o canal de comunicação a ser utilizado pelo Titular de Dados em caso de dúvidas sobre o consentimento.

vi. Fluxo automatizado de envio do Termo de Consentimento aos Titulares de Dados informados, por e-mail, para aceitação ou rejeição do termo;

vii. Captura automática da resposta dos Titulares de Dados sobre a aceitação ou rejeição do termo e a data de resposta, para controle de expiração do consentimento;

viii. Possibilidade de se consultar consentimentos já obtidos por finalidade e/ou Titular de Dados e se obter o prazo de validade de cada consentimento;

ix. Possibilidade de se indicar a revogação do consentimento a partir de uma solicitação formal do Titular (integração com Portal do Titular).

e) Possuir módulo de análise situacional automatizada de adequação à LGPD, contendo as seguintes funcionalidades:

i. A partir das informações já cadastradas e associadas na solução, realizar diagnósticos automatizado das informações e, a partir dessa análise, gerar riscos e/ou

atividades de adequação, considerando as seguintes regras:

- Processos de negócio
  - Para cada processo ainda não aprovado, gerar atividade de aprovação do processo;
  - Para cada processo sem modelagem associada, gerar atividade de modelagem do processo;
- Ativos da informação
  - Para cada ativo da informação sem responsável, gerar atividade de se definir responsável pelo ativo;
  - Para cada ativo sem medida técnica de segurança associada, gerar atividade de se estudar as medidas técnicas de segurança associadas ao ativo e um risco de vulnerabilidade do ativo;
  - Para cada ativo sem medida técnica de prevenção associada, gerar atividade de se estudar as medidas técnicas de prevenção associadas ao ativo e um risco de vulnerabilidade do ativo;
  - Para cada ativo com nível de confiabilidade "baixo", gerar atividade de melhoria de medidas técnicas do ativo e um risco de vulnerabilidade do ativo;
  - Para cada ativo cadastrado sem um processo associado, cadastrar uma atividade de revisão das informações do ativo;
  - Para cada ativo cadastrado sem artefato associado, cadastrar uma atividade de revisão das informações do ativo;
- Artefatos
  - Para cada artefato cadastrado sem tratamento de dados associado, gerar uma atividade de revisão das informações do artefato;
  - Para cada artefato cadastrado sem metadados pessoais cadastrados, gerar uma atividade de revisão das informações do artefato;

- Metadados pessoais e tratamentos de dados pessoais e bases legais
  - Para cada metadado pessoal cadastrado que seja do tipo "sensível" e estiver associado a um tratamento de dados com base legal de "legítimo interesse do controlador", criar uma atividade de revisão do tratamento do dado e um risco indicando a realização de tratamento de dado sensível sem a devida base legal;
  - Para cada tratamento de dado pessoal cadastrado que não tenha informações sobre origem/destino dos dados em tratamento, criar uma atividade de revisão da atividade de tratamento;
  - Para cada tratamento de dado pessoal cadastrado que tenha como base legal o consentimento do titular e não possua informações sobre o processo de consentimento, criar uma atividade de revisão do processo de consentimento e um risco de tratamento de dados sendo realizado sem o devido consentimento do titular;
  - Para cada tratamento de dado pessoal cadastrado que trate dados de crianças e adolescentes e não tenha um processo de consentimento definido, criar uma atividade de revisão do tratamento e um risco de tratamento de dados de criança/adolescente sendo realizado sem o devido consentimento do pai/responsável;
  - Para cada tratamento de dado pessoal cadastrado que utilize fundamentação legal ou regulatória como base legal e não tenha a indicação dessa fundamentação, gerar uma atividade de análise do tratamento e um risco que indique a realização de tratamento de dados sem a devida base legal adequadamente informada;

- Para cada tratamento de dado pessoal cadastrado que tenha indicado o processamento dos dados através de rotinas automatizadas, sem a intervenção humana, gerar uma atividade de análise impacto sobre essa rotina;
- Para cada tratamento de dado pessoal cadastrado que não possua processo de descarte ou prazo de armazenamento, gerar uma atividade de revisão da atividade de tratamento e um risco sobre a realização de tratamento de dados por tempo indeterminado;
- Para cada tratamento de dado pessoal cadastrado que não possua metadados pessoais associados, gerar uma atividade de revisão das informações sobre a finalidade de tratamento;
- Para cada tratamento de dado pessoal cadastrado que utilize o legítimo interesse do controlador como base legal, gerar uma atividade de revisão da rotina de tratamento e um risco indicando a fragilidade do tratamento por ser justificado apenas pelo legítimo interesse do controlador;
- Para cada tratamento de dado pessoal cadastrado que possua metadados pessoais associados que não sejam indicados como imprescindíveis para o objetivo do tratamento, gerar uma atividade para revisão da rotina de tratamento e um risco indicando o tratamento de dados pessoais sem cumprimento do princípio da necessidade (inciso III, Art. 6º da LGPD);
- Para cada tratamento de dado pessoal cadastrado que esteja apontada como executada por um Operador e não houver contrato com o Operador associado à finalidade, gerar uma atividade para revisão contratual e um risco indicando o gap jurídico;

- Medidas técnicas de segurança
  - Para cada medida técnica de segurança cadastrada que não possua uma medida administrativa associada, criar uma atividade de revisão das medidas para inclusão do relacionamento das medidas técnicas e administrativas de segurança e um risco que indique que há medidas técnicas de segurança implementadas que não aparecem definidas em nenhuma medida administrativa de segurança;
  - Para cada medida técnica de segurança cadastrada que não possua nenhuma associação com qualquer ativo da informação, criar uma atividade de revisão dos cadastros de medidas técnicas e ativos da informação;
- Medidas administrativas de segurança
  - Para cada medida administrativa cadastrada que não contenha anexo, gerar uma atividade de revisão da medida técnica e um risco de falta de documentação da medida administrativa;
  - Se não houver nenhuma medida de administrativa externa cadastrada, gerar um risco de falta de medida administrativa com foco externo;
  - Se não houver nenhuma medida administrativa interna cadastrada, gerar um risco de falta de medida administrativa com foco interno;
  - Se houver medida administrativa cadastrada com data de vigência já extrapolada, gerar uma atividade de revisão da medida e um risco de medidas inválidas em uso;
  - Para cada medida administrativa cadastrada que não possua a indicação de um processo de manutenção da medida, criar uma atividade de revisão/criação de rotina de manutenção da medida

e um risco sobre a dificuldade de manutenibilidade da medida;

- Para cada medida administrativa cadastrada que não possua indicativo que ela esteja integrada à Gestão de Governança Corporativa do controlador, gerar uma atividade de revisão dessa medida e um risco que indique que há medidas administrativas em uso que não integram a governança corporativa do controlador;
- Se não houver nenhuma medida administrativa cadastrada onde esteja indicado um desses parâmetros como "verdadeiro", gerar uma atividade para revisão das medidas administrativas de segurança e um risco que trate da gestão dos compromissos assumidos pelo controlador:
  - A medida trata o papel do Titular e seus direitos;
  - A medida trata o papel do Encarregado de Proteção de Dados;
  - A política trata o papel do controlador e operador;
  - A medida trata riscos de privacidade;
  - A medida trata o processo de incidentes e notificação no caso de violação de dados pessoais;
  - A medida trata o processo de transferência/compartilhamento de dados pessoais.

- Contratos com terceiros
  - Para cada contrato cadastrado que não contenha anexo, gerar uma atividade de revisão do contrato um risco de falta de documentação de contratos;
  - Se não houver nenhuma medida de administrativa externa cadastrada, gerar um risco de falta de medida administrativa com foco externo;

- Se não houver nenhum contrato com clientes e/ou operadores cadastrado, gerar uma atividade de revisão do inventário dos contratos;
- Para cada contrato cadastrado que não possua indicativo que suas cláusulas de privacidade estejam integradas à Gestão de Governança Corporativa do controlador, gerar uma atividade de revisão desse contrato e um risco que indique que há cláusulas contratuais em uso que não integram a governança corporativa do controlador;
- Se o contrato cadastrado não possuir indicado um desses parâmetros como "verdadeiro", gerar uma atividade para revisão do contrato e um risco que trate das cláusulas contratuais do controlador:
  - O contrato trata as medidas administrativas de segurança;
  - O contrato trata tópicos das medidas técnicas de segurança;
  - O contrato trata sobre tratamento de dados pessoais;
  - O contrato trata sobre o ciclo de vida dos dados pessoais em tratamento.

- Riscos
  - Para cada risco cadastrado que tenha sua criticidade definida como "Alta", criar uma atividade de gestão do risco;
  - Para cada risco cadastrado que tenha uma data de disparo, mas não esteja com status "encerrado" ou "cancelado", criar uma atividade de gestão do risco;
  - Para cada risco que não tenha um descritivo da estratégia a ser utilizada para a gestão do risco, criar uma atividade de gestão do risco;
  - Para cada risco que tenha como probabilidade de ocorrência com valor maior do que 85%, gerar uma atividade de gestão do risco;

- Para cada risco que não tenha associado a ele um processo, tratamento de dado pessoal ou ativo, criar uma atividade de revisão/gestão do risco.

f) Possuir módulo de indicadores de negócio, contendo as seguintes funcionalidades:

i. Possibilidade de criação de dashboards e indicadores eletrônicos que cruzem qualquer dado gerenciado pela solução;

ii. Possibilidade de compartilhamento dos indicadores via aplicativo e e-mail;

iii. Possibilidade de manutenção de dashboards e seus indicadores;

iv. Possibilidade de publicação dos dashboards e seus indicadores dentro das interfaces de qualquer módulo da solução, em formato .HTML, sem a necessidade de codificação.

4.5.5. A solução deverá ser disponibilizada para um total de 10 (dez) usuários nominais da CONTRATANTE por um período de 12 (doze) meses.

5. FATORES QUALITATIVOS DOS SERVIÇOS

5.1. Os serviços tratados no projeto descrito neste documento são complexos e envolvem equipes multidisciplinares especialistas, atuando paralelamente em atividades muitas vezes codependentes entre si.

5.2. O sucesso do projeto, então, se dará pelo atendimento de todos os requisitos detalhados anteriormente neste documento, bem como a um controle qualitativo da gestão do projeto, a ser realizado pela equipe da CONTRATADA.

5.3. Visando garantir o bom andamento das atividades do projeto e maximizar os resultados esperados, estabelece-se que a gestão do projeto deverá ocorrer, no mínimo, de acordo com as etapas a seguir:

5.3.1. Time da CONTRATADA

a) A CONTRATADA deverá alocar um time de especialista suficiente para atender a todas as atividades planejadas para o projeto e produzir todos os produtos de trabalhos detalhados neste Termo de Referência;

b) A equipe da CONTRATADA deve, em conjunto, possuir todas as habilidades técnicas necessárias para a execução dos serviços e deve ser composta pelos seguintes papéis:

i. *Gerente de Projetos*: Papel responsável pela gestão completa do projeto; ponto focal entre a CONTRATADA e CONTRATANTE;

ii. *Encarregado de Proteção de Dados (DPO)*: Papel responsável pelas definições técnicas e decisões finais sobre todos os aspectos técnicos relacionados à adequação à LGPD; não executará atividades de DPO (Encarregado) em nome da CONTRATANTE, mas será a referência técnica do projeto para o restante da equipe da CONTRATADA e da CONTRATANTE;

iii. *Analista de Processos*: Papel responsável por realizar o levantamento, desenho (em notação BPMN 2.0) e atividades de implantação e capacitação de processos de negócio (AS-IS e TO-BE) durante o curso do projeto;

iv. *Analista LGPD*: Papel responsável por realizar o levantamento inventário, análises e definições relacionadas aos produtos de trabalho diretamente associados à LGPD do projeto;

v. *Analista de Tecnologia da Informação*: Papel responsável por realizar o levantamento, inventário, análises e definições relacionadas às medidas técnicas de segurança de ativos de TI tratadas no projeto;

vi. *Analista jurídico*: Papel responsável por realizar o levantamento, inventário e análises relacionadas a hipóteses e bases legais de tratamento de dados pessoais e riscos jurídicos associados à LGPD durante o curso do projeto.

c) Caberá à CONTRATADA definir o quantitativo ideal de pessoal para cada papel, visando atender as demandas do projeto, de acordo com o quantitativo limite de horas estabelecidos por cada item do objeto;

d) A equipe da CONTRATADA deverá ser liderada por um Gerente de Projetos responsável por ser o ponto focal entre o Fiscal do Contrato da CONTRATANTE e o restante da equipe;

e) O Gerente de Projetos da CONTRATADA deverá gerenciar todas as etapas do projeto descritas neste documento;

f) A equipe destacada pela CONTRATADA deverá se liderada por profissionais que atendam aos requisitos definidos a seguir, no tópico 6.4;

g) A CONTRATANTE irá definir um Fiscal do Contrato para ser o par do Gerente de Projetos da CONTRATADA internamente;

h) O Fiscal do Contrato será responsável por ser o ponto focal entre o Gerente de Projetos da CONTRATADA, a equipe da CONTRATADA e toda a equipe da CONTRATANTE;

i) O Fiscal do Contrato irá facilitar o acesso da CONTRATADA às informações da CONTRATANTE necessárias para a correta execução das atividades e irá colocar à disposição da equipe da CONTRATADA todos os colaboradores da CONTRATANTE necessários para que seja possível se realizar o levantamento de informações, validação de produtos de trabalho criados e atividades de capacitação;

j) O Fiscal do Contrato irá assinar, mensalmente, todos os Relatórios Mensais de Atividades produzidos pela CONTRATADA e será o responsável pelas medições do projeto e autorizações para faturamento.

5.3.2. Planejamento do projeto

a) Após a autorização para início do projeto, a CONTRATADA deverá criar um Plano de Projeto detalhado, a ser apresentado pelo Gerente de Projetos à CONTRATANTE;

b) O Plano de Projeto deve conter todos os parâmetros a serem observados durante toda a execução contratual e irá servir como guia para alinhamento de expectativas entre as partes;

c) No mínimo os seguintes temas deverão ser abordados no Plano de Projeto, sempre em concordância com os parâmetros definidos neste Termo de Referência:

i. Escopo do trabalho a ser realizado;

ii. Estimativa de consumo de horas para cada atividade, por tipo de objeto;

iii. Produtos de trabalho a serem entregues;

iv. Cronograma detalhado;

v. Equipe do projeto (papéis e responsabilidades);

vi. Plano de comunicação;

vii. Riscos do projeto e plano de gestão desses riscos;

viii. Principais referências (modelos e padrões) que serão utilizados pela CONTRATADA para execução dos serviços;

ix. Ferramentas que serão utilizadas no projeto;

x. Procedimentos a serem adotados para cada etapa de gestão do projeto.

d) As atividades técnicas do projeto somente poderão ser iniciadas após aprovação do Plano de Projeto pela CONTRATANTE, ação que deverá ocorrer em uma reunião presencial entre as partes, a ser realizada na sede da CONTRATANTE, onde será realizado o *Kick-off do Projeto*, que resumirá os parâmetros definidos no Plano de Projeto para apreciação e aprovação do Fiscal do Contrato.

5.3.3. Acompanhamento e medição do projeto

a) Todas as atividades técnicas realizadas pela CONTRATADA no âmbito do projeto deverão ser devidamente documentadas e demonstradas à CONTRATANTE como evidência da execução dos serviços, criando assim lastro para os faturamentos financeiros a serem executados;

b) Nenhum faturamento deverá ser realizado pela CONTRATADA sem que haja respectivas evidências de prestação de serviços e entregas de produtos de trabalhos associados a ele;

c) Caberá à CONTRATADA elaborar, mensalmente, um Relatório Mensal de Atividades em que deverá listar todas as atividades realizadas durante o período, o consumo de horas por tipo de objeto relacionado à atividade, e produtos de trabalho entregues à CONTRATANTE, resultado dessas atividades;

d) As informações constantes no Relatório Mensal de Atividades darão subsídio ao Fiscal do Contrato para a aferição da prestação de serviços, medição das entregas em relação ao Plano de Projeto e em relação aos parâmetros financeiros do projeto, em concordância com o Cronograma Físico-Financeiro estimado para o projeto;

e) O Relatório Mensal de Atividades deverá também listar os riscos em aberto até o momento no projeto, as estratégias de gestão desses riscos e qualquer pendência que precise ser tratada a seguir para que o projeto possa alcançar seus objetivos, bem como as principais decisões tomadas entre as partes para resolução de *issues* ou mesmo para execução de estratégias operacionais do projeto relacionados ao período;

f) Dessa forma, haverá transparência e alinhamento de expectativas documentados quanto ao projeto, permitindo que as partes possam sempre ter um único *baseline* de informações gerenciais;

g) Mensalmente, antes do faturamento, o Gerente de Projeto da CONTRATADA deverá apresentar o Relatório Mensal de Atividades ao Fiscal do Contrato para aprovação e, após aprovação formal do documento, a CONTRATADA poderá então emitir Nota Fiscal relacionada às atividades e entregas documentadas ali no documento.

5.3.4. Gestão de mudanças

a) Durante a execução dos serviços é provável que existam alterações ou mudanças do planejamento do projeto,

motivadas por novos fatos, aprendizados, conflito de agendas e uma série de outros eventos naturais de um cenário complexo como o tratado aqui;

b) As mudanças podem endereçar, entre outras, as seguintes alterações no projeto:
   i. Atualização no cronograma de atividades;
   ii. Atualização de agendas e ordem de atividades;
   iii. Atualização do quadro de pessoal do projeto;
   iv. Atualização do plano de comunicação do projeto;
   v. Ajuste de escopo (mantendo sempre observância ao objeto do projeto);
   vi. Ajuste de parâmetros de produtos de trabalho (como ordem de produção, detalhamento de suas informações, tamanho do artefato em relação ao projeto, etc.).

c) Todas as mudanças do projeto deverão ser gerenciadas formalmente para que não se perca o controle do projeto;

d) Para que uma determinada mudança do Plano de Projeto possa valer como novo estado do projeto, a mesma deverá ser gerenciada de acordo com o seguinte procedimento:
   i. A parte responsável por observar a necessidade da mudança deve documentá-la em uma Solicitação de Mudança, onde a alteração deve ser detalhada e justificada;
   ii. A Solicitação de Mudança deve ser apresentada à outra parte para análise e aprovação;
   iii. Uma vez aprovada, a Solicitação de Mudança deve ser divulgada a todos os envolvidas no projeto e documentada no Relatório Mensal de Atividades do período. A partir daí, os termos da Solicitação de Mudança passam a valer no projeto;
   iv. Caso a Solicitação de Mudança não seja aprovada pelas 2 (duas) partes, ela não terá validade no projeto e deverá ser arquivada.

5.3.5. Encerramento

a) Após o fim da execução das atividades técnicas previstas no projeto (tratadas aqui e detalhadas no Plano de Projeto), a CONTRATADA deverá executar rotinas para o encerramento formal do projeto;

b) O encerramento do projeto deverá ser documentado em um Termo de Encerramento de Projeto, que deverá ser analisado e assinado pelo Fiscal do Contrato e pelo Gerente de Projetos;

c) O Termo de Encerramento de Projeto irá marcar o aceite definitivo dos serviços prestados e resumir as entregas realizadas pela CONTRATADA à CONTRATANTE durante todo o curso do projeto;

d) Após a elaboração e assinatura do Termo de Encerramento do Projeto, a CONTRATADA estará liberada de suas atribuições técnicas do projeto e poderá desalocar sua equipe;

e) Caberá à CONTRATANTE, após a assinatura do Termo de Encerramento do Projeto, emitir à CONTRATADA um Atestado de Capacidade Técnica, detalhando as atividades cumpridas durante o projeto;

f) Todos os faturamentos associados ao projeto deverão ocorrer antes da emissão do Termo de Encerramento do Projeto.

6. CAPACITAÇÃO TÉCNICA DAS PROPONENTES

6.1. Visando dar garantias quanto à qualidade dos serviços prestados e, consequentemente, dos resultados esperados do projeto, a PMIS define que as proponentes deverão comprovar aptidão para a prestação dos serviços a serem contratados.

6.2. Essa comprovação deverá ocorrer a partir da demonstração de atestados de competência técnica, expedidos por outros clientes da proponente, sejam eles da esfera pública ou privada, que demonstrem a execução prévia dos seguintes serviços realizados pela proponente:

6.2.1. Execução de projetos de implementação de governança de privacidade, em conformidade com a Lei Geral de Proteção de Dados (LGPD);

6.2.2. Mapeamento de processos de negócio em notação BPMN;

6.2.3. Execução de atividades de implantação das ferramentas ofertadas;

6.2.4. Licenciamento e entrega da solução ofertada;

6.2.5. Atividades de gerenciamento de projetos.

6.3. Além disso, a proponente também deverá comprovar, previamente à assinatura do contrato, que seu time técnico possui conhecimentos específicos e especializados nas principais disciplinas tratadas no projeto.

6.4. A comprovação da competência técnica do time da proponente deverá ocorrer a partir da demonstração das seguintes certificações profissionais de parte da equipe que irá atuar no projeto:

6.4.1. Ao menos 1 (um) colaborador, exclusivamente, deverá possuir a certificação *EXIN DPO Certified*, demonstrando sólidos conhecimentos em tópicos de adequação e operação da LGPD;

6.4.2. Ao menos 1 (um) colaborador, exclusivamente, deverá possuir certificação ABPMP CBPP ou similar, demonstrando sólidos conhecimentos em modelagem e gestão de processos de negócio;

6.4.3. Ao menos 1 (um) colaborador, exclusivamente, deverá possuir certificação ISO/IEC 27.001, demonstrando sólidos conhecimentos em tópicos e segurança da informação.

6.5. Considerando o caráter operacional, tecnológico e jurídico de alta complexidade do projeto, e a realidade heterogênea administrativa da CONTRATANTE, as proponentes deverão também realizar *visita técnica* nas dependências da PMIS para ter contato direto com a realidade da CONTRATANTE e sanar todas as dúvidas em relação ao projeto e ao cenário da PMIS.

6.5.1. A visita técnica deverá ser realizada, obrigatoriamente, em até 24 (vinte e quatro) horas antes da sessão do certame licitatório e deverá ser agendada com até 48 (quarenta e oito) horas de antecedência através do canal definido no instrumento convocatório.

6.5.2. Após a realização da visita técnica, a CONTRATANTE irá emitir um atestado de visita técnica que deverá ser apresentado pela proponente juntamente com as comprovações de capacitação técnica descritas anteriormente, sob pena de desclassificação.

6.6. Após finalizada a etapa administrativa do processo licitatório, a vencedora do pregão deverá demonstrar que a solução ofertada por ela

atende aos requisitos estabelecidos neste projeto através da realização de uma *prova de conceito*.

6.6.1. Os requisitos da prova de conceito foram definidos no tópico 12 deste Termo de Referência.

7. Local de Execução

7.1. As interações entre CONTRATADA e CONTRATANTE poderão ser realizadas de forma remota, visando minimizar custos de deslocamentos desnecessários;

7.2. Quando for percebido pela CONTRATANTE ou CONTRATADA a necessidade da realização de atividades presenciais, essas ações deverão ser planejadas previamente entre as partes e ocorrerão na sede da CONTRATANTE, localizada no endereço:

7.2.1. Av. Eduardo Roberto Daher, 1135 – Itapecerica da Serra - SP

7.2.2. Horário: Dias úteis, das 09:00 às 16:00

7.3. Caso haja necessidade de deslocamentos para outros endereços da CONTRATANTE, esses endereços serão repassados em tempo de projeto e todos os deslocamentos ocorrerão, de qualquer forma, dentro dos limites do município;

7.4. Atividades técnicas como análises, produção de produtos de trabalho, configurações, e qualquer outra que não envolva, diretamente, colaboradores da CONTRATANTE poderão também ser realizadas de forma remota, ou na sede da CONTRATADA, desde que isso não traga nenhum prejuízo aos resultados esperados para o projeto;

7.5. Isso não exclui eventuais necessidades de reuniões presenciais a serem realizadas para tratativas de cenários distintos do projeto, sempre que houver necessidade apontada por qualquer uma das partes. Nesse caso, esses eventos deverão ocorrer dentro das instalações da CONTRATANTE.

8. Premissas e Restrições

8.1. Para que o projeto seja executado adequadamente e os resultados esperados sejam alcançados, devem ser considerados os seguintes

parâmetros como premissas e restrições a serem observados durante todo o curso da prestação dos serviços:

8.1.1. Caberá à CONTRATANTE

a) Proporcionar todas as facilidades para a CONTRATADA desempenhar o fornecimento do objeto do presente Termo de Referência, permitindo o acesso dos profissionais da CONTRATADA às suas dependências e fornecendo todas as informações reais necessárias para a execução dos serviços;

b) Indicar e manter um colaborador responsável pela fiscalização e o acompanhamento do bom andamento dos serviços contratados;

c) Manter controle dos limites de horas disponíveis para cada tipo de objeto;

d) Facilitar a comunicação entre o time da CONTRATADA e o time da CONTRATANTE alocados no projeto;

e) Executar ou providenciar a execução, com urgência, dos serviços de sua responsabilidade para que não prejudiquem a execução dos trabalhos da CONTRATADA;

f) Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas neste Termo de Referência;

g) Promover o acompanhamento e a fiscalização do objeto do presente Termo de Referência, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas.

8.1.2. Caberá à CONTRATADA

a) Ser responsável por todas as obrigações e encargos previdenciários, fiscais, trabalhistas e comerciais da execução do CONTRATO com a CONTRATANTE;

b) Alocar no projeto profissionais devidamente capacitados e habilitados para a realização dos serviços especificados neste documento, impondo-lhes rigoroso padrão de qualidade, segurança e eficiência, correndo por sua conta todas as despesas com salários, impostos, contribuições

previdenciárias, encargos trabalhistas, seguros e outras despesas correlatas;

c) Emitir, sempre que solicitado pela CONTRATANTE, relatórios gerencias e/ou técnicos referentes aos serviços realizados;

d) Apresentar Relatório Mensal de Atividades, junto com a fatura de serviços prestados, relacionando todas as entregas realizadas no período para a CONTRATANTE e demais relatórios que ratifiquem a execução dos serviços prestados;

e) Manter controle dos limites de horas disponíveis para cada tipo de objeto;

f) Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços, bem como, prestar esclarecimentos que forem solicitados pela CONTRATANTE;

g) Acatar integralmente todas as regras de sigilo, privacidade e segurança da informação impostas pela CONTRATANTE a partir da assinatura do contrato de prestação de serviços.

9. CRONOGRAMA ESTIMADO

9.1. Buscando equilibrar a urgência da adequação à LGPD e seus prazos legais, e a complexidade do projeto de adequação, a CONTRATANTE define como restrição que o projeto tenha duração de 12 (doze) meses, a ser executado de acordo com o cronograma estimado a seguir:

Item do objeto	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12
Diagnóstico situacional (*gap analysis*) da LGPD	13%	13%	13%	13%	13%	13%	13%	9%				
Reengenharia de processos de negócio visando adequação à LGPD								15%	25%	25%	25%	10%
Implantação de novos processos de negócio visando adequação à LGPD									25%	25%	25%	25%
Capacitação sobre LGPD	10%								15%	25%	25%	25%
Disponibilização de ferramentas LGPD	8%	8%	8%	8%	8%	8%	8%	8%	9%	9%	9%	9%

9.2. O cronograma em questão poderá sofrer alterações de acordo com o planejamento detalhado do projeto por parte da CONTRATADA e de

acordo com fatos que certamente serão observados durante a execução do projeto.

9.3. Mesmo assim, qualquer alteração que se faça necessária no cronograma aqui proposto deverá:

9.3.1. Ser discutida entre as partes e aprovada, em última instância, pela CONTRATANTE;

9.3.2. Buscar maximizar os resultados do projeto;

9.3.3. Respeitar o prazo limite de 12 (doze) meses de execução, exceção feita apenas por motivos de força maior a ser discutido entre as partes;

9.3.4. Ser considerado válido apenas após o cumprimento dos trâmites administrativos da CONTRATANTE e aprovado pelo Fiscal do Contrato.

10. QUANTITATIVOS PREVISTOS PARA O PROJETO

10.1.1. Para a realização do projeto, estima-se o consumo de horas técnicas de serviço a serem disponibilizadas por cada tipo de objeto, e o licenciamento da solução ofertada de acordo com o quantitativo de usuários nominais da CONTRATANTE, conforme tabela a seguir:

#	Item	Unidade	Quantitativo
1	Diagnóstico da situação atual da Governança de Privacidade	Horas técnicas	5.000
2	Reengenharia operacional para implementação de Programa de Governança de Privacidade	Horas técnicas	2.000
3	Implantação de processos adicionais para Programa de Governança de Privacidade	Horas técnicas	250
4	Treinamento e Capacitação sobre Governança de Privacidade	Horas técnicas	150
5	Implantação de soluções tecnológicas de Governança de Privacidade	Usuários	10

11. MODELO DE PROPOSTA DO PROJETO

À Prefeitura do Município de Itapecerica da Serra/SP

#	Serviços	Unidade	Quantidade	Valor unitário	Subtotal
1	Diagnóstico da situação atual da Governança de Privacidade	Horas técnicas	5.000	R$	R$
2	Reengenharia operacional para implementação de Programa de Governança de Privacidade	Horas técnicas	2.000	R$	R$
3	Implantação de processos adicionais para Programa de Governança de Privacidade	Horas técnicas	250	R$	R$
4	Treinamento e Capacitação sobre Governança de Privacidade	Horas técnicas	150	R$	R$
5	Implantação de soluções tecnológicas de Governança de Privacidade	Usuários	10	R$	R$
Proposta total (*)					**R$**

(*) No valor total da proposta estão inclusos todos os custos diretos e indiretos envoltos na prestação dos serviços e disponibilização das ferramentas do projeto, incluindo: salários, encargos sociais, encargos trabalhistas, vale-transporte, vale-refeição e qualquer outra despesa com pessoal, infraestrutura, deslocamento e impostos associados.

Proposta total por extenso: _____

Validade da proposta: 90 dias

Prazo de execução dos serviços: 12 (doze) meses

Dados do proponente:

Razão social: _____

CNPJ: _____

Endereço: _____

Nome do contato: _____

E-mail: _____ Telefone: _____

Data, local

_____

Assinatura

12. PROVA DE CONCEITO

12.1. Como definido anteriormente, todo o trabalho técnico especializado a ser executado durante o curso do projeto deverá culminar em informações inventariadas e associadas em uma solução tecnológica de Governança de Privacidade.

12.2. Para garantir que a solução proposta pela proponente atenda aos requisitos estabelecidos no projeto, a empresa vencedora da fase de lances do processo licitatório deverá submeter a solução proposta a uma avalição por parte do time técnico da CONTRATANTE.

12.3. Essa prova de conceito será realizada nas dependências da CONTRATANTE em um prazo de até 3 (três) dias após o resultado do processo licitatório.

12.4. Na ocasião da prova de conceito, a proponente deverá demonstrar os requisitos aqui estabelecidos para uma comissão avaliadora da CONTRATANTE, sob pena de desclassificação em caso de não comparecimento e/ou descumprimento de qualquer um dos requisitos.

12.5. O objetivo dessa validação é dar garantias à CONTRATANTE dos aspectos qualitativos da arquitetura, funcionalidades e de critérios de segurança da solução.

12.6. Na sessão da prova de conceito a proponente deverá apresentar toda a documentação exigida e, na sequência, realizar a navegação da solução e demonstrar, de forma prática, todos os requisitos definidos a seguir.

12.7. Durante a demonstração de requisitos que não sejam explicitamente documentais, não serão aceitos a exibição de vídeos, slides ou qualquer outra mídia multimídia ou estática.

12.8. A CONTRATANTE irá avaliar cada requisito listado e, após um prazo de até 5 (cinco) dias úteis, irá emitir um relatório com o resultado da demonstração, aprovando ou não a solução ofertada.

12.9. As demais licitantes participantes do certame poderão acompanhar a prova de conceito, mas não poderão se manifestar, exceto pelos meios oficiais e definidos no Edital quanto a recursos ou demais apontamentos, tal como definido em Lei.

12.10. A proponente convocada para a realização da prova de conceito terá apenas 1 (uma) tentativa para realizar sua demonstração, sem a chance de nova tentativas.

12.11. A CONTRATANTE irá fornecer, na sessão de prova de conceito, apenas link de internet, energia e um meio de exibição (TV ou retroprojetor), e será de responsabilidade da proponente fornecer os demais equipamentos e softwares necessários para a execução da demonstração.

12.12. Durante a demonstração só serão aceitas atividades de codificação, configuração ou instalação das soluções (em todo ou parte) quando o requisito a ser demonstrado definir isso de forma explícita; ou seja, caberá à proponente trazer e demonstrar uma solução que atenda aos requisitos "pronta" e funcional.

12.13. Iniciada a prova de conceito, a proponente terá um prazo de até 4 (quatro) horas para realizar a demonstração, cabendo a ela fazer uso desse prazo da forma que melhor lhe convier, inclusive em relação à ordem de apresentação dos requisitos.

12.14. Durante a realização da prova de conceito, não será permitida a substituição de nenhum componente de hardware ou de software utilizado pela proponente.

12.15. Os requisitos demonstrados e atendidos de forma "parcial" não serão considerados atendidos. Dessa forma, caberá à proponente demonstrar na integralidade todos os requisitos aqui dispostos, uma vez que eles já endereçam apenas uma porção do total dos requisitos detalhados no projeto.

12.16. A solução demonstrada será considerada aprovada se todos os requisitos listados a seguir forem demonstrados integralmente, sem erros ou bugs.

12.17. A solução demonstrada será considerada reprovada se qualquer um dos requisitos listados a seguir não for demonstrado de forma integral, ou apresentarem qualquer tipo de erro ou bug; ou se a proponente não comparecer na sessão de prova de conceito agendada.

12.18. Durante a execução da prova de conceito, a proponente deverá demonstrar o cumprimento integral dos seguintes requisitos:

#	Requisito	Critério de aceite
1	A equipe da proponente que irá realizar a prova de conceito deve ser devidamente apresentada e ter sido autorizada formalmente pela empresa licitante	Apresentação de uma procuração que identifique os colaboradores da proponente e de a eles poderes e autorização para a realização da prova de conceito em nome da licitante.
2	A solução demonstrada deve ser identificada e apesentada formalmente à CONTRATANTE	Apresentação de um documento que identifique os aspectos de identificação, arquiteturais, técnicos, funcionais e de versão de todos os softwares e hardwares utilizados durante a prova de conceito.
3	A solução demonstrada deve estar hospedada em um ambiente de nuvem seguro, que possua padrões de qualidade comprovados nos quesitos de gerenciamento de serviços de TI	Apresentação de certificação ISO/IEC 20.000, ou compatível, da plataforma que sustenta a solução demonstrada.
4	A solução demonstrada deve estar hospedada em um ambiente de nuvem seguro, que possua padrões de qualidade comprovados nos quesitos de segurança da informação	Apresentação de certificação ISO/IEC 27.001, ou compatível, da plataforma que sustenta a solução demonstrada.
5	A solução demonstrada deve estar hospedada em um ambiente de nuvem seguro, que possua padrões de qualidade comprovados nos quesitos de privacidade	Apresentação de certificação ISO/IEC 27.701, ou compatível, da plataforma que sustenta a solução demonstrada.
6	A solução demonstrada deve ter um acordo de nível de serviço que garanta disponibilidade de, no mínimo, 98%	Apresentação de documentação emitida pelo fabricante da plataforma que sustenta a solução que demonstre o Acordo de Nível de Serviço (ANS) atendendo a padrões de disponibilidade de até 98%, com regras estabelecidas para sanções em caso de quebra do acordo.
7	A solução demonstrada deve ser totalmente web e acionada tanto via browser como via aplicativo	Demonstração de acesso e navegação geral de cada módulo da solução em browser e aplicativo móvel. A exceção se dá para o módulo de atendimento aos direitos dos titulares, quando acessado pelo Titular de Dados, que não precisa ser acessado via aplicativo.
8	A solução demonstrada deve possuir fluxos de aprovação automatizados customizáveis, sem a necessidade de codificação	Apresentação do módulo de configuração de fluxos automáticos de informação e demonstração prática de 1 (um) fluxo já configurado e modificação deste fluxo sem se utilizar de codificação.
9	A solução demonstrada deve possuir a capacidade de exportar e importar dados através de planilhas em formato .XLSX sem a necessidade de codificação adicional	Apresentar o processo de exportação de informações de ao menos quaisquer 30 (trinta) itens (metadados pessoais, processos, ativos, artefatos, riscos, etc.) previamente cadastrados na solução para planilhas em formato .XLSX e apresentação da planilha gerada com o mesmo conteúdo presente na solução.
10	Possuir cadastro de pessoas envolvidas no projeto incluindo nome, e-mail e foto	Demonstrar a criação de 1 (um) novo usuário com todos os atributos listados no requisito.
11	Possuir cadastro de processos de negócio, com possibilidade de cadastro de modelagem BPMN navegável gráfica (em formato .HTML) para cada processo	Demonstrar o cadastro de 1 (um) processo de negócio incluindo uma modelagem BPMN navegável, em formato .HTML ao processo cadastrado. A proponente poderá fazer uso de uma modelagem previamente criada e já cadastrada na plataforma apresentada.

#	Requisito	Critério de aceite
12	Possuir cadastro de Ativo incluindo o cadastro de análise de confiabilidade da informação de cada ativo da informação, permitindo cadastro independente de características de Confidencialidade, Integridade e Disponibilidade das informações tratadas pelo ativo e possibilidade de categorização automática do nível de confiabilidade do ativo de acordo com a classificação de cada item da CID de informação do ativo	- Demonstrar o cadastro de 1 (um) ativo da informação associado a um processo de negócio cadastrado; - Demonstrar a definição automática do parâmetro de nível de confiabilidade do ativo de acordo com as mudanças dos parâmetros de confidencialidade, integridade e disponibilidade associados ao ativo.
13	Possuir cadastro de artefatos tratados por cada ativo da informação cadastrado, com diferenciação do tipo de titular de dados que tem seus dados pessoais tratados no Ativo (munícipe, fornecedor/operador, colaborador do controlador)	Demonstrar a criação de 1 (um) novo artefato com todos os atributos listados no requisito, e associado a um determinado ativo cadastrado.
14	Possuir cadastro de metadado pessoal, tratado em cada artefato previamente cadastrado e possibilidade de classificação do metadado pessoal compatível com o Decreto Federal nº 10.046/19	Demonstrar a criação de ao menos 3 (três) metadados pessoais associados a artefatos cadastrados. Os metadados devem ser classificados de acordo com os tipos: - Biográfico; - Cadastral; - Biométrico.
15	Possuir cadastro de tratamentos de dados pessoais com possibilidade de indicação da base legal/hipótese de tratamento da LGPD (Arts. 7º e 11º da LGPD) associada e possibilidade de indicação de fundamentação legal associada à finalidade (Lei ou Decreto);	Demonstrar o cadastro de 2 (dois) tratamentos de dados pessoais observando as seguintes regras: - O tratamento 1 deve estar associada a uma hipótese prevista da LGPD que indique uma lei ou decreto externo; - O tratamento 1 deve ser associada a um fundamento legal externo previamente cadastro; - O tratamento 1 deve estar associada a um artefato cadastrado na solução. - O tratamento 2 deve estar associada a uma hipótese prevista da LGPD que a necessidade de consentimento do titular; - O tratamento 2 não deve estar associada a nenhum artefato.
16	Tratar a possibilidade de se associar um artefato e seus metadados pessoais a um tratamento de dados pesoais com indicação se essa associação atende ou não ao princípio da Necessidade do tratamento de Dados (inciso III do Art. 6º da LGPD);	Demonstrar a indicação de que um determinado metadado não é imprescindível para a realização do tratamento de dado pessoal previsto no tratamento 1 tratado no requisito #15.

#	Requisito	Critério de aceite
17	Possuir cadastro de medidas administrativas de segurança (políticas) com possibilidade de se anexar documentos e realizar uma análise qualitativa automática dos principais parâmetros de cada medida administrativa cadastrada	Demonstrar a criação de uma medida administrativa (política) com os seguintes atributos: - Título; - Data de publicação e vigência; - Tipo (interna ou externa); - Anexo (qualquer tipo de arquivo de documento); - Parâmetros qualitativos que mostrem informações sobre os seguintes aspectos da medida: - completude; - exequibilidade; - integração da política com a governança do controlador.
18	Possuir cadastro de contratos com titulares e operadores com possibilidade de se anexar documentos e realizar uma análise qualitativa automática dos principais parâmetros de cada contrato cadastrado	Demonstrar a criação de 1 (um) contrato com os seguintes atributos: - Título; - Data de início e fim de vigência; - Tipo (com operador ou não); - Terceiro associado ao contrato; - Associação a um determinado artefato cadastrado na solução; - Tratamento de dados pessoal associado ao contrato; - Anexo (qualquer tipo de arquivo de documento); - Parâmetros qualitativos que mostrem informações sobre os seguintes aspectos do contrato: - se trata de medidas administrativas de segurança; - se trata de medidas técnicas de segurança.
19	Possuir fluxo automatizado de aviso para tratamento de riscos cadastrados/disparados	Demonstrar a criação de 1 (um) risco por completo, incluindo a indicação dos seguintes atributos: - probabilidade de ocorrência; - impacto; - criticidade; - descrição; - responsável; - tratamento de dado pessoal associado; - ativo associado. Disparar o risco e demonstrar que o responsável pelo risco recebeu a informação sobre o disparo do risco por e-mail, de forma automática.
20	Possuir fluxo automatizado de aviso para atividades de adequação cadastradas/encerradas	Demonstrar a criação manual de 1 (uma) atividade de adequação à LGPD associada a um tipo específico de assunto, com os seguintes atributos: - Descrição da atividade; - Data de início; - Data fim; - Pessoal executora (utilizar qualquer pessoa previamente cadastrada no projeto); - Status; - Tipo de atividade. Após a criação da atividade, demonstrar que o executor associado recebeu um e-mail, automaticamente, o informando do cadastro da atividade.

#	Requisito	Critério de aceite
21	Possuir cadastro de Titulares no Portal do Titular com validação de autenticidade do Titular com foto	Demonstrar o cadastro de 1 (um) Titular de Dados, incluindo uma rotina de autenticação, conforme segue: - Titular solicita cadastro e informa nome, e-mail e uma chave de identificação do tipo CPF; - Titular anexa foto de documento; - Titular anexa foto segurando o documento; - Titular acessa portal e, por ainda não ter seu cadastro validado, não tem acesso ao cadastro de solicitações.
22	Permitir que o Encarregado de Proteção de Dados (DPO) realize a aprovação de cadastros solicitados no Portal dos Titulares mediante comprovação de autenticidade	Demonstrar que o DPO recebeu a solicitação do Titular cadastrada no requisito #21 e demonstrar a execução dos passos de aprovação: - DPO recebe solicitação de cadastro; - DPO consulta informações e anexos enviados pelo Titular para comprovar autenticidade; - DPO autoriza cadastro; - Titular recebe e-mail automático com autorização de cadastro; - Titular realiza login após cadastro e obtém acesso ao cadastro de solicitações.
23	Permitir o cadastro de nova solicitação de um Titular de Dados, dividida por tipo de solicitação (solicitação de informação, pedido de revogação de consentimento, solicitação de atualização de dados, solicitação de esquecimento, outros)	- Demonstrar a criação de 1 (uma) solicitação de um determinado tipo qualquer por parte do titular; - Demonstrar o recebimento automático, na fila de solicitações ao DPO, da nova solicitação do Titular, com os mesmos parâmetros e informações definidas pelo Titular; - Demonstrar que o DPO recebeu um e-mail automático contendo a solicitação.
24	Permitir o recebimento de e-mail automático quando houve resposta a cada uma das solicitações do Titular feitas no Portal do Titular	- Demonstrar o fluxo de resposta do DPO à solicitação criada no requisito #23; - Demonstrar que o Titular, após resposta do DPO, recebeu retorno de sua solicitação de forma automática, via e-mail; - Demonstrar que o Titular tem acesso ao histórico de suas solicitações no portal, após login com sucesso.
25	Possuir cadastro de tipos de solicitações de Titular de Dados com definição de SLA máximo para cada tipo de solicitação	Demonstrar a possibilidade de o DPO realizar o cadastro de 2 (dois) tipos de solicitações possíveis de serem feitas pelo Titular, com os seguintes atributos: - Título; - Prazo de SLA do tipo de solicitação.
26	Tratar o cadastro de Incidentes de segurança com possibilidade de se associar riscos e ativos previamente cadastrados a cada incidente	Demonstrar o cadastro de 1 (um) novo incidente de segurança associado a um risco já cadastrado.
27	Possuir cadastro de Notificação a partir de um Incidente previamente cadastrado que tratou da violação de dados pessoais	- Demonstrar a criação de uma nova notificação a partir do cadastro do incidente realizado no requisito #26, de forma automática, herdando as informações do risco para o incidente. - Demonstrar a possibilidade de se diferenciar notificações a serem enviadas à ANPD e aos Titulares de Dados.

#	Requisito	Critério de aceite
28	Permitir a geração automática do documento de notificação (em formato .pdf) para ANPD de acordo com os requisitos determinados pela ANPD.	- Demonstrar a geração do arquivo em formato .PDF de 1 (uma) notificação contendo no mínimo os seguintes atributos: • Remetente; • Destinatário; • Data do envio; • Título da notificação • Data do incidente associado; • Descrição do incidente associado; • Descrição do risco associado (se houver); • Tratamentos de dados pessoais associados ao incidente; • Ativos de informação associados; • Medidas técnicas associadas aos ativos associados; • Natureza dos dados pessoais envolvidos no incidente; • Detalhes dos titulares de dados envolvidos; • Medidas adotadas para mitigar os efeitos do incidente; • Motivos para demora da notificação. - Demonstrar o armazenamento do arquivo da notificação na solução para futura consulta.
29	Executar envio de e-mail da notificação aos Titulares de Dados, com controle de data de envio e guarda da cópia das notificações enviadas.	- Demonstrar a criação de 1 (uma) notificação que inclua o envio a Titulares de Dados; - Demonstrar que, ao acionar a realização do envio a Titulares de Dados, a plataforma realiza o envio automaticamente e registra o envio realizado em uma lista de envios realizados; - Demonstrar que o e-mail foi recebido, automaticamente, no endereço de 1 ou mais Titulares de Dados associados à notificação e que a notificação possui, ao menos, os atributos listados no critério de aceite do requisito #28 e filtra os dados pessoais apenas para o titular envolvido.
30	Possuir módulo de Gestão de Consentimento que gere Termos de Consentimentos a partir da possibilidade de se selecionar tratamento de dados pessoal, previamente cadastrado, que utiliza como hipótese de tratamento/base legal o consentimento do Titular	Demonstrar a possibilidade de se selecionar os tratamentos de dados pessoais previamente cadastrados que tenham como base legal/hipótese de tratamento o consentimento do titular e solicitar a geração automática dos Termos de Consentimento.

#	Requisito	Critério de aceite
31	Realizar a criação automática do Termo de Consentimento contendo as seguintes informações: • Processo de negócio envolvido no consentimento (associado ao tratamento selecionado); • Tratamento de dados pessoais associado ao consentimento; • Indicação se o tratamento realiza o compartilhamento dos dados com terceiros; • Indicação dos detalhes do compartilhamento dos dados com terceiros, se esse for o caso; • Lista de metadados pessoais associados ao tratamento selecionado; • Link para a política de privacidade do controlador; • Prazo de validade do consentimento; • Detalhes sobre o canal de comunicação a ser utilizado pelo Titular de Dados em caso de dúvidas sobre o consentimento.	- Acionar a geração do Termo de Consentimento para 1 (um) tratamento de dado pessoal cadastrado que usa o consentimento como base legal/hipótese de tratamento de dados pessoais e está classificada como tratamento que compartilha os dados com terceiros. - Demonstrar que as informações de processo, tratamento, metadados pessoais e compartilhamento com terceiros são carregadas automaticamente na geração do consentimento. - Demonstrar os demais parâmetros do consentimento no Termo gerado. - Demonstrar o Termo de Consentimento gerado e enviado por e-mail, automaticamente, a um Titular de dados específico. - Demonstrar o recebimento do Termo de Consentimento por e-mail ao Titular de Dados. - Demonstrar o OK do Titular de Dados ao Consentimento, feito a partir do corpo do próprio e-mail. - Demonstrar o recebimento e armazenamento do consentimento na plataforma, contendo data da obtenção do consentimento e data de expiração final.
32	Tratar a possibilidade de se indicar a revogação do consentimento a partir de uma solicitação formal do Titular (integração com Portal do Titular)	- Demonstrar a lista de consentimentos obtidos, (incluindo o consentimento criado no requisito #31), consultar o status do consentimento como "válido"; - Criar uma solicitação de revogação de um consentimento pela ótica do Titular; - Demonstrar o recebimento do pedido de revogação do consentimento; - Demonstrar a atualização do status do consentimento para "revogado", com data da revogação igual à data atual do sistema.
33	Possuir módulo de análise situacional automatizada de adequação à LGPD que analisa o inventário de ativos, garantindo que para cada ativo com nível de confiabilidade "baixo", seja gerada, automaticamente, uma atividade de melhoria de medidas técnicas do ativo e um risco de vulnerabilidade do ativo	- Demonstrar que há ativos da informação cadastrados que possuam nível atual de confiabilidade definidos como "baixo"; - Demonstrar que não há atividades e riscos associados a esse ativo previamente cadastrados; - Acionar o módulo de análise situacional e demonstrar que, após análise automática, foi criada uma atividade específica para melhoria das medidas técnicas do ativo em questão (identificável) e que foi criado um risco de vulnerabilidade específico para o mesmo ativo.
34	Possuir módulo de análise situacional automatizada de adequação à LGPD que analisa o inventário de artefatos, garantindo que para cada tratamento de dado pessoal cadastrado que não possua metadados pessoais associados, seja gerada, automaticamente, uma atividade de revisão das informações sobre a finalidade de tratamento	Acionar o módulo de análise situacional e demonstrar que, após análise automática, foi criada ao menos 1 (uma) nova atividade específica para revisão de algum tratamento de dado pessoal previamente cadastrado que não possua metadados pessoais associados a ele.

#	Requisito	Critério de aceite
35	Possuir módulo de análise situacional automatizada de adequação à LGPD que analisa o inventário de tratamentos de dados pessoais, garantindo que para cada tratamento cadastrado que possua metadados pessoais associados que não sejam indicados como imprescindíveis para o objetivo do tratamento, seja gerada, automaticamente, uma atividade para revisão da rotina de tratamento e um risco indicando o tratamento de dados pessoais sem cumprimento do princípio da necessidade (inciso III, Art. 6º da LGPD)	Acionar o módulo de análise situacional e demonstrar que, após análise automática, foi criada ao menos 1 (uma) nova atividade específica para revisão de algum tratamento de dado pessoal previamente cadastrado que possua metadados pessoais associados a ele, mas que existem metadados pessoais que não estejam marcados como imprescindíveis para cumprimento da finalidade do tratamento. Demonstrar que, para o mesmo tratamento de dado pessoal detectado, foi criado 1 (um) novo risco associado ao tratamento e que enderece risco de não cumprimento do princípio da necessidade.
36	Possuir módulo de análise situacional automatizada de adequação à LGPD que analisa o inventário de medidas administrativas de segurança, garantindo que para, caso haja medida administrativa cadastrada com data de vigência já extrapolada, seja gerada, automaticamente, uma atividade de revisão da medida e um risco de medidas inválidas em uso	Acionar o módulo de análise situacional e demonstrar que, após análise automática, foi criada ao menos 1 (uma) nova atividade específica para revisão de alguma política previamente cadastrada que tenha sido expirada. Demonstrar que foi criado 1 (um) novo risco que enderece a vigência vencida da política.
37	Possuir módulo de análise situacional automatizada de adequação à LGPD que analisa o inventário de riscos, garantindo para que cada risco cadastrado que tenha sua criticidade definida como "Alta", seja gerada, automaticamente, uma atividade de gestão do risco	Acionar o módulo de análise situacional e demonstrar que, após análise automática, foi criada ao menos 1 (uma) nova atividade específica que enderece a gestão de 1 (um) risco previamente cadastrado e classificado com criticidade "Alta".
38	Possuir módulo de indicadores de negócio que permita a publicação dos dashboards e seus indicadores dentro das interfaces de qualquer módulo da solução, em formato .HTML, sem a necessidade de codificação	Demonstrar a exibição de 3 (três) indicadores quaisquer que sejam criados a partir de dados cadastrados na solução em browser e em aplicativo, com possibilidade de interação do usuário nos componentes dos indicadores.
39	Possuir módulo de indicadores de negócio que permita a publicação dos dashboards e seus indicadores dentro das interfaces de qualquer módulo da solução, em formato .HTML, sem a necessidade de codificação	- Demonstrar a alteração de ao menos 1 (um) indicador previamente cadastrado no painel exibido, sem a necessidade de codificação; - Demonstrar a atualização do painel após modificação.

ANDREA REJANE DE ASSIS
Secretária
Secretaria Municipal de Administração

RONE VAZ DA SILVA
Assessor Geral
Secretaria Municipal de Governo e Tecnologia