Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

1. **OBJETIVO**

1.1. Descrever Sistema de Registro de Preços para Contratação de empresa para o **fornecimento de solução tecnológica de apoio na adequação às obrigações da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, com prestação de 12 meses**, em conformidade com a Lei nº 10.520/2002 (Regulamenta o art. 37, inciso XXI, da Constituição Federal, para instituir a modalidade de licitação denominada pregão), com aplicação subsidiária da Lei nº 8.666/1993 (Regulamenta o art. 37, inciso XXI, da Constituição Federal, que institui normas para licitações e Contratos da Administração Pública e dá outras providências), com o Decreto Estadual nº 46.642/2019 (Regulamenta a fase preparatória das contratações no âmbito do Estado do Rio de Janeiro) e o Decreto Estadual nº 46.751/2019 (regulamenta o Sistema de Registro de Preços no art. 15 da Lei Federal nº 8.666/1993).

1.2. A licitação será realizada na modalidade *PREGÃO EM SUA FORMA ELETRÔNICA*, nos termos da Lei n.º 10.520/2002, do Decreto Estadual n.º 46.751/2019 que regulamenta o Sistema de Registro de Preços e da Lei n.º 8.666/ 1993 .

1.3. Forma de Adjudicação do Objeto: *MENOR PREÇO GLOBAL POR LOTE.*

1.4. Forma de Execução do Objeto: *EMPREITADA POR PREÇO UNITÁRIO.*

2. **JUSTIFICATIVA**

2.1. Dotar o PRODERJ com capacidade para gerenciar e aplicar as novas diretrizes de tratamento de dados pessoais com foco em *compliance* de proteção de dados para adequação à Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), de modo a resguardar e preparar as medidas efetivas e necessárias para que o órgão esteja aderente aos princípios previstos da LGPD.

2.2. O PRODERJ é Autarquia vinculada à Secretaria de Estado de Transformação Digital - SETD, na forma do Decreto Estadual nº 48.151/2022 e atua como Órgão Gestor do Sistema Estadual de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro - SETIC/RJ, com competência dada pelo art. 5º do Decreto Estadual nº 47.278/2020.

2.3. O PRODERJ é responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, as bases de dados de vários órgãos estaduais e os diversos equipamentos hospedados no *Data Center* do Estado. É responsável também por prover serviços de *Internet* aos órgãos da Administração Estadual, tais como correio eletrônico, consultoria, desenvolvimento, hospedagens de páginas, portais, *intranets* e *extranets*.

2.4. Considerando a importância vital dos sistemas e serviços de TIC da Administração Pública e os dados pessoais tratados por esses sistemas, a contratação de serviços para apoiar a gestão e *compliance* com a LGPD torna-se mandatória.

2.5. Há de ressaltar, porém, que a reduzida equipe de segurança do PRODERJ composta pelos membros da DGD - Diretoria de Governança e Dados e Informações e da DSI- Diretoria de Segurança da Informação, bem como a ausência de uma solução que permita dar segurança no cumprimento da LGPD impedem que se assegure infraestrutura apropriada às atividades e disponibilidade de sistemas essenciais de TIC à Administração.

2.6. A importância de o PRODERJ possuir uma gestão eficiente e abrangente em relação à LGPD, além de atendimento à norma em apreço, decorre de suas competências institucionais enquanto órgão gestor do SETIC/RJ, bem como, frente às disposições do art. 9º do Decreto Estadual nº 47.826/2021 - *que instituiu o Comitê Estadual de Governança e Privacidade de Dados no âmbito do Estado.*

2.7. Não menos importante é a competência do PRODERJ para propor Registro de Preços em contratações de bens e serviços relativos à TIC, para o atendimento das demandas dos demais órgãos da Administração Pública, por força do art. 4°, §2° do Decreto Estadual n° 46.751/2019.

2.8. Sabendo-se que a informação é um dos ativos mais importantes e caros do mundo corporativo, seja no âmbito público ou privado, a proteção dessas informações, ante a irreversível informatização dos acervos corporativos de dados, exige cada vez mais o uso de soluções eficazes em tecnologia da informação, que auxiliem na gestão adequada dos dados pelos órgãos públicos.

2.9. A reserva de informações à disposição do poder público requer providências preparatórias para adequações contidas na Lei de proteção de dados – Lei n° 13.709/2018.

2.10. Dito isso, pretende-se por meio do presente Termo de Referência, com base nos estudos preliminares realizados, viabilizar a contratação de solução tecnológica para adequação à LGPD.

3. **ALINHAMENTO ESTRATÉGICO**

3.1. A contratação em tela está alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2023, conforme abaixo:

a) **Objetivo Estratégico 1** – Proporcionar soluções e melhorias aos serviços de TIC oferecidos aos cidadãos: Proporcionar serviços de TIC adequados aos cidadãos, buscando oportunidades de melhoria contínua, identificando lições aprendidas e avaliando o real valor agregado destes serviços (objetivo orçamentário alinhado com as ações 1293, 1294 e 4477 do PPA);

b) **Objetivo Estratégico 4** – Implementar a Governança de TIC do estado: Definir os processos e controles necessários à aplicação da Governança de TIC, tendo como diretriz o foco nos processos prioritários, simplificação com eficácia e contato com os usuários internos, órgãos públicos estaduais e o mercado (objetivo orçamentário alinhado com as ações 4133 e 4508 do PPA);

c) **Objetivo Estratégico 7** - Promover o processo de Segurança da Informação e Comunicação: Implementar o processo, revisar normas, monitorar os incidentes de segurança e disseminar a cultura da segurança da informação, junto aos servidores do PRODERJ e demais órgãos da administração pública estadual (objetivo não orçamentário).

3.2. Também encontra alinhamento estratégico com o Plano Pluri-Anual (PPA) 2020-2023, registrada com os códigos de ação nº 1293 (atualização tecnológica do parque computacional), n° 1294 (atualização tecnológica dos sistemas de informação) n° 4477 (desenvolvimento e inovação em tecnologia digital), respectivamente nos códigos do produto nº 6884 (ferramenta de segurança da informação implantada), nº 6826 (ferramenta automatizada de segurança adquirida) e nº 6917 (inovação tecnológica implantada).

3.3. Por fim, a contratação para o presente objeto, está prevista no PCA- Plano de Contratações Anual.

4. **DOTAÇÃO ORÇAMENTÁRIA**

No caso concreto, fica dispensada a indicação de prévia dotação orçamentária no sistema de registro de preços, uma vez que esta será exigida tão somente quando da efetivação da respectiva contratação.

5. **RESULTADOS ESPERADOS**

5.1. Em primeiro plano, cumprir a legislação é condição obrigatória imposta a de todos os órgãos públicos.

5.2. Espera-se com a presente contratação dotar o PRODERJ e demais órgãos da administração com recursos tecnológicos necessários às boas práticas de segurança , com infraestrutura adequada e ainda:

a) Diagnosticar necessidades de adequação, propor e executar medidas para adequar o órgão contratante à Lei 13.709/2018 e demais padrões de segurança recomendados para órgãos da administração pública;

b) Identificar processos que realizam tratamento de dados pessoais e adequá-los aos requisitos da Lei 13.709/2018;

c) Apoiar os órgãos da administração pública, direta e indireta, em conjunto com o Comitê Estadual de Governança e Privacidade de Dados, tanto junto ao Núcleo Normativo quanto ao Núcleo Executor;

d) Mitigar o risco da ocorrência de incidentes de segurança que representem violações de dados e implementar processos para tratamento de incidentes e violações de dados, caso ocorram;

e) Aperfeiçoar os requisitos de transparência quando do tratamento de dados pessoais nos serviços prestados ao cidadão;

f) Implementar processo de Governança em Privacidade de Dados Pessoais;

g) Identificar e gerir riscos à privacidade;

h) Implementar processos para gestão de consentimento e preferências;

i) Gerir requisições dos titulares de dados pessoais;

j) Disseminar a cultura de privacidade no âmbito dos órgãos e entidades da Administração Pública por meio de treinamentos e campanhas de conscientização;

k) Apoiar, se necessário, o Encarregado pelo Tratamento de Dados Pessoais, na implementação e manutenção da Governança em Privacidade de Dados Pessoais, em processo de melhoria contínua.

6. **DEMANDA ESTIMADA E QUANTITATIVO**

6.1. A tabela abaixo apresenta a estrutura da plataforma digital do PRODERJ, sobretudo, dos quantitativos de servidores e de bancos de dados que correspondem aos ativos de dados a serem tratados e protegidos pela solução, conforme apurado nos estudos preliminares.

SOLUÇÃO LGPD - LOTE				
ITEM	**ID SIGA**	**DESCRIÇÃO**	**MÉTRICA**	**QUANTIDADE ESTIMADA**
1	177603	Subscrição de solução de gestão para adequação e governança de conformidade com a LGPD, incluindo suporte técnico e atualização de software pelo período de 12 meses	unidade	1
2	177604	Subscrição de solução de descoberta e mapeamento de dados estruturados e não estruturados, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade	100
3	177605*	Subscrição de Solução de Descoberta e Monitoramento de Dados Não Estruturados, com Suporte Técnico e Atualização de Software (**Subscrição de solução para conscientização e treinamento em segurança e privacidade, incluindo suporte técnico e atualização do software pelo período de 12 meses**)	unidade	1.400
4	176272	Subscrição de solução de Gestão de Atendimento a Titulares, Denúncias e Governança de Certificados em conformidade com a LGPD, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade	25
5	177644	Treinamento na Solução de Gestão LGPD	aluno	16
6	177646	Serviço de consultoria para apoio na implementação das soluções e adequação à LGPD	UST	24.096
* para o item 3, ID SIGA/RJ: 177605, considerar a descrição entre parênteses.				

6.2. Para a definição dos quantitativos a serem demandados, necessários ao cumprimento dos objetivos propostos para a Contratação, buscou-se utilizar parâmetros comuns utilizados como referência nas contratações similares observadas neste Termo de Referência, adaptando-os para um modelo flexível e que permita ao PRODERJ contratar os serviços nas quantidades que venham a ser efetivamente necessárias.

6.3. Tal medida levou em consideração o fato de que em alguns casos, o quantitativo necessário só será descoberto no decorrer da execução, uma vez que o PRODERJ possui em sua plataforma de dados, servidores e bancos de dados que vieram juntamente com os servidores recebidos pela Autarquia, frutos de legado olímpico e sobre os quais não há conhecimento acerca dos dados, seja em termos de quantidades, seja em termos de qualidade ou natureza.

6.4. Saliente-se que, o presente objeto, assim como outros já contratados como, por exemplo, a ferramenta de Data Loss Prevention (DLP) ou a de gerenciamento de chaves criptográficas (anonimização de dados) irão, cada um dentro de suas características e atuações, viabilizar ao PRODERJ obter essa visibilidade sobre parte significativa dos ativos de dados sob sua guarda, dos quais não tem maiores informações.

6.5. Desta forma, buscou-se definir para cada item do objeto, métricas e quantidades que estejam adequadas às necessidades do PRODERJ e que sirvam como parâmetro para a precificação por parte das empresas licitantes interessadas no fornecimento do objeto.

6.6. De acordo com o levantamento realizado, cujos números são apresentados na tabela acima, o PRODERJ apresenta as seguintes estimativas, conforme cada item componente da solução proposta à contratação:

O item 01 é o principal componente de software do objeto e compreende ao elemento gerenciador da solução. Uma única licença cobre toda uma plataforma de dados e, conforme a estrutura e tamanho, poderá ser complementado com a contratação dos itens 2 a 4;

O item 02 é o componente da solução cuja estimativa está relacionada com a quantidade de bancos de dados a serem tratados, onde uma unidade corresponde a uma instância de banco de dados ou fonte de dado estruturado e não-estruturado. Cada unidade é aplicável a até 120 unidades de bancos de dados aproximadamente, conforme cada fabricante desta solução. Assim, considerando o quantitativo de BD's (vide tabela acima), projetou-se uma demanda de até 100 unidades para este item, ao longo de 12 meses;

O item 03 é o componente da solução aplicável aos usuários nos diversos eventos de conscientização e treinamento ao longo de 12 meses, sendo certo que usuário corresponde a cada indivíduo alvo das ações (conscientização / treinamento);

O item 04 é componente da solução aplicável às repartições da estrutura corporativa do contratante, sendo cada unidade aplicável a até duas áreas. Considerando que o PRODERJ possui aproximadamente 50 repartições em sua estrutura, foi estimado o quantitativo de 25 unidades para este item;

O item 05, que trata do treinamento, deverá abordar todos os componentes da solução contratada, orientando sua correta utilização e funcionamento, bem como orientando acerca da configuração, utilização e administração dos recursos. A métrica por aluno viabiliza treinar e capacitar exatamente o número necessário de servidores que, após treinados, poderão atuar também como replicadores/facilitadores dos conteúdos aprendidos. Nesse passo, considerando que o objeto tem aderência a quatro repartições do PRODERJ, a saber: Diretoria de Governança e Dados e Informações (Encarregado de Dados Pessoais), Diretoria de Segurança da Informação, Diretoria de Sistemas e Soluções e Diretoria de Infraestrutura, definiram-se 4 vagas por área para capacitação na solução contratada, totalizando as 16 vagas previstas para demanda;

Para fins de medição das UST referentes ao item 6 (serviço de consultoria especializada) foi considerada uma estimativa de frequência de eventos pertinentes a cada um dos itens, a partir do levantamento realizado pela DGD/PRODERJ, conforme se infere do Catálogo de Serviços anexado ao presente Termo de Referência (anexo II).

6.7. Após a realização de Plano de suprimentos (PLS SIGA nº 0147/2023) o quantitativo estimado para a contratação passou a ser o seguinte:

LOTE PARA SOLUÇÃO DE LGPD

ITEM	ID SIGA	DESCRIÇÃO	MÉTRICA	QUANTIDADE ESTIMADA
1	177603	Subscrição de solução de gestão para adequação e governança de conformidade com a LGPD, incluindo suporte técnico e atualização de software pelo período de 12 meses	unidade	22
2	177604	Subscrição de solução de descoberta e mapeamento de dados estruturados e não estruturados, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade	600
3	177605*	Subscrição de Solução de Descoberta e Monitoramento de Dados Não Estruturados, com Suporte Técnico e Atualização de Software (Subscrição de solução para conscientização e treinamento em segurança e privacidade, incluindo suporte técnico e atualização do software pelo período de 12 meses)	unidade	19.120
4	176272	Subscrição de solução de Gestão de Atendimento a Titulares, Denúncias e Governança de Certificados em conformidade com a LGPD, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade	104
5	177644	Treinamento na Solução de Gestão LGPD	aluno	276
6	177646	Serviço de consultoria para apoio na implementação das soluções e adequação à LGPD	UST	181.840
* para o item 3, ID SIGA/RJ 177605, considerar a descrição entre parênteses.				

6.7.1. **Quantidades estimadas por órgão participante**

Órgão Participante	LOTE					
	ID 177603	ID 177604	ID 177605	ID 176272	ID 177644	ID 177646
DETRO - - Departamento de Transportes Rodoviários do Estado do Rio de Janeiro Rua Uruguaiana, 118, 8º andar, Centro - Rio de Janeiro/RJ	1	0	200	2	2	4.728
EMOP - Empresa de Obras Públicas do Estado do Rio de Janeiro Campo de São Cristóvão, 138, São Cristóvão - Rio de Janeiro/RJ	1	25	420	4	2	6.728
CGE - Controladoria Geral do Estado do Rio de Janeiro Avenida Erasmo Braga, 118 - 12º e 13º andar - Setor: DGAF - Rio de Janeiro/RJ	1	25	800	6	5	6.872
JUCERJA - Junta Comercial do Estado do Rio de Janeiro Av. Rio Branco, 10, 7º ANDAR. Centro - Rio de Janeiro/RJ	1	0	200	2	12	4.160
IEEA - Instituto Estadual de Engenharia e Arquitetura Rua Campo de São Cristóvão, 138, 2º andar - São Cristóvão, Rio de Janeiro/RJ	1	0	100	2	2	4.256
SEGOV - Secretaria de Estado de Governo Rua Pinheiro Machado, s/n, Laranjeiras, Rio de Janeiro/RJ	1	0	400	4	12	5.088
FAETEC - - Fund de Apoio à Escola Técnica do Estado do Rio de Janeiro Endereço de acordo com o órgão	1	25	800	2	16	8.136
CEPERJ - Fund Centro Est. Estat. Pesq. Serv RJ Av. Carlos Peixoto, 54 Sala 304, Botafogo - Rio de Janeiro/RJ	1	25	550	6	12	8.480
SEPM - Secretaria de Estado de Polícia Militar Rua Carmo Neto, s/nº, Prédio CICC - Bairro Cidade Nova, Rio de Janeiro/RJ	1	25	800	6	25	8.064
PRODERJ - Centro de Tecn de Informação e Comunicação do Estado do Rio de Janeiro Rua da Conceição, 69. 24 e 25 andares. Centro - Rio de Janeiro/RJ	1	100	1.400	25	16	19.760
FAF - Fundo Especial de Adm Fazendária Av. Presidente Vargas, 670, Centro - Rio de Janeiro/RJ	1	25	800	6	30	7.824
RIOPREVIDENCIA - Fundo Único de Previdência do Estado do Rio de Janeiro Rua da Quitanda, 106, Centro - Rio de Janeiro/RJ	1	25	550	6	18	8.472
SES - Secretaria de Estado de Saúde Endereço de acordo com o órgão	1	100	3.200	6	30	14.384
SEEDUC - Secretaria de Estado de Educação Endereço de acordo com o órgão	1	100	2.500	6	40	14.888
SECC - - Secretaria de Estado da Casa Civil Rua Pinheiro Machado, s/nº - Laranjeiras - Rio de Janeiro/RJ	1	25	800	4	19	8.016
GSI - Gabinete de Segurança Institucional do Governo do Estado do Rio de Janeiro R. Pinheiro Machado, s/nº - Laranjeiras, Rio de Janeiro/RJ	1	25	350	2	10	8.544
IRM - Instituto Rio Metrópole R. Benedito Hipólito - Cidade Nova, Rio de Janeiro - RJ	1	0	50	1	10	4.784
SEAP - Secretaria de Estado de Administração Penitenciária Endereço de acordo com o órgão	1	0	1.300	0	2	4.936
AGENERSA - Agência Reguladora de Energia e Saneamento do Estado do Rio de Janeiro Endereço de acordo com o órgão	1	0	200	2	2	5.304
DETRAN - Departamento de Trânsito do Estado do Rio de Janeiro Endereço de acordo com o órgão	1	50	800	6	4	13.784
DPGE - Defensoria Pública Geral do Estado Endereço de acordo com o órgão	1	0	2.100	5	5	6.808
PROCON - Proteção e Defesa do Consumidor Endereço de acordo com o órgão	1	25	800	1	2	7.824
TOTAL	**22**	**600**	**19.120**	**104**	**276**	**181.840**

6.8. **Quantitativo máximo para adesões**

LOTE						
Ocorrência	**ID 177603**	**ID 177604**	**ID 177605**	**ID 176272**	**ID 1776044**	**ID 177646**
Quantidade máxima de aquisição por meio de adesão	44	1.200	38.240	208	552	363.680
Quantidade máxima de aquisição por órgão aderente	11	300	9.560	52	138	90.920

6.8.1. Os endereços dos órgãos participantes, para fins de cumprimento do objeto, constam na tabela do subtópico 6.7.1.

7. **REQUISITOS PARA A CONTRATAÇÃO**

7.1. **Requisitos Objetivos**

7.1.1. Dotar o PRODERJ e demais órgãos interessados na contratação com capacidade para gerenciar e aplicar as novas diretrizes de tratamento de dados pessoais, com foco em *compliance* de proteção de dados para adequação à Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

7.1.2. Dotar o PRODERJ e demais órgãos com os recursos tecnológicos necessários às boas práticas de segurança.

7.2. **Necessidades Tecnológicas Básicas**

Para atender a demanda em exame, os recursos tecnológicos deverão considerar as seguintes necessidades e requisitos básicos:

I - **Necessidade 1: Gerenciar o mapeamento, descoberta, classificação e tratamento dos dados:**

a) Realizar o tratamento dos dados conforme a LGPD descreve: tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

II - **Necessidade 2: Gerenciar requisições de acesso aos dados do titulares – DSAR (Data Subject Access Request):**

a) Receber e gerenciar as requisições dos titulares de modo que o titular dos dados obtenha do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, informação acerca dos dados gerenciados pelo órgão contratante;

b) Realizar o controle de prazos de pedidos e respostas, padronizar e automatizar respostas, de modo a facilitar o fluxo de resposta ao titular dos dados.

III - **Necessidade 3: Gerenciar a comunicação resposta acerca sobre incidentes e violações de segurança:**

a) Gerenciar a resposta dos incidentes de forma centralizada, de forma a automatizar o tratamento destes incidentes;

b) Gerenciar a comunicação para autoridade nacional e ao titular sobre a ocorrência de incidentes e(ou) violações de segurança que possam acarretar riscos ou danos relevantes aos titulares;

c) Automatizar avisos de violação às leis de proteção de dados, permitindo realizar as notificações de forma eficaz.

IV - **Necessidade 4: Gerenciar o consentimento do usuário**

a) Gerenciar e manter a guarda dos dados de solicitação, fornecimento e revogação de consentimento feitas pelo titular dos dados;

b) Gerenciar o fornecimento de consentimento pelo titular dos dados, ressalvadas as hipóteses, previstas na Lei, de dispensas de consentimento;

c) Integrar solicitação e fornecimento de consentimento com aplicações em geral e com aplicativos (apps) para dispositivos móveis, incluindo a gestão de Cookies utilizados nas páginas de websites, possibilitando a integração com os sites de forma controlar seu consentimento por meio de banner personalizável.

V - **Necessidade 5: Permitir integração com ferramentas/plataformas de anonimização de dados:**

a) Permitir a integração para anonimização dos dados de forma que os dados do titular não possam ser identificados, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

VI - **Necessidade 6: Dispor de serviços de consultoria para apoio na implantação das soluções e adequação à LGPD:**

a) Prover serviço técnico de apoio no processo de implantação e sustentação dos serviços contratados;

b) A força de trabalho para a prestação dos serviços deverá possuir e demonstrar sua capacidade operacional, por meio de apresentação de certificados de capacitação, emitidos por empresa credenciada, quando couber;

c) Configuração, parametrização e operação da ferramenta;

d) Monitorar o desempenho da solução;

e) Executar tarefas de operação assistida da ferramenta;

f) Garantir a operação segura e efetiva da solução;

g) Executar tarefas orientativas e consultivas;

h) Apoiar e gerenciar a definição e mapeamento de processos de Realizar anonimização de dados de acordo com as necessidades do órgão contratante;

i) Apoiar e gerenciar o Mapeamento, a Descoberta, a Classificação e o Tratamento dos Dados;

j) Apoiar e gerenciar as requisições de acesso aos dados do Titulares – DSAR (Data Subject Access);

k) Apoiar e gerenciar o consentimento do usuário.

VII - **Necessidade 7: Treinamento para uso da Solução:**

a) Deverá ser fornecido treinamento oficial abarcando o conteúdo necessário para a perfeita compreensão e operação de todos os requisitos da solução;

b) Ao final do treinamento, deverá ser fornecido um certificado de conclusão, contendo as seguintes informações mínimas: nome do curso, nome do instrutor, carga horária total e ementa do treinamento.

VIII - **Necessidade 8: Abertura de chamados de Suporte Técnico:**

a) As soluções disponibilizadas, quando necessário, deverão possuir suporte técnico com atendimento remoto/presencial para solução de quaisquer problemas que impeçam o funcionamento adequado;

b) Deverão ser fornecidas atualizações tecnológicas de correções de erros e/ou de melhorias nas soluções disponibilizadas, quando necessário, além das bases de conhecimento;

c) Deverá existir mecanismo adequado para abertura e acompanhamento de chamados de suporte técnico, 24h por dia, 7 dias por semana, 365 dias por ano.

IX - **Necessidade 9: Manutenção do Sigilo das Informações:**

a) Os relatórios gerados deverão ser classificados quanto ao sigilo das informações;

b) Os servidores/colaboradores que tiverem acesso às informações contidas nos relatórios deverão assinar termo de sigilo, a fim de se evitar exposição de riscos e possíveis vulnerabilidades que possam afetar a autenticidade, integridade, disponibilidade e confidencialidade dos ativos de TIC do órgão contratante.

7.3. **Necessidades Socioambientais**

A empresa contratada deverá adotar prática de sustentabilidade ambiental na execução do objeto, quando couber, conforme critérios estabelecidos no Decreto Estadual nº 43.629/2012.

7.4. **Aderência a Padrões e Modelos**

Não se aplica.

7.5. **Recursos Materiais e Humanos**

7.5.1. Os materiais didáticos para treinamento serão disponibilizados conforme informações constantes neste Termo de Referência.

7.5.2. Quaisquer outros materiais e/ou acessórios necessários ao pleno funcionamento da solução contratada, não previstos, deverão ser fornecidos pela licitante vencedora, sem custos adicionais para a contratante.

7.5.3. Em observação do Enunciado nº 14, item 5 da Procuradoria Geral do Estado do Rio de Janeiro - PGE/RJ, e também considerada a Portaria PRODERJ/PRE nº 942/2022, saliente-se que o objeto da presente contratação não prevê mão de obra residente nas dependências do órgão contratante. Adicionalmente registre-se que o objeto também não caracteriza, de forma alguma, terceirização de atividade fim da Autarquia, tendo em vista que se trata de solução tecnológica e serviços técnicos de suporte em LGPD, que estão diretamente relacionados à atuação de profissionais técnicos, não se confundindo com as atividades inerentes aos servidores da Autarquia, que não possui em seus quadros e no plano de cargos vigente, profissional técnico ou analista com qualificação para atender o objeto em tela.

7.5.4. Não se aplica ao objeto deste contrato o fornecimento de uniformes ou equipamentos de proteção individual (EPI).

7.6. **Necessidades de Negócio**

7.6.1. **Suporte Técnico e Atualização de Software**

7.6.1.1. As seguintes especificações de suporte técnico e atualização deverão ser adotadas paras os itens 1 a 4:

I - A Contratada deverá disponibilizar suporte técnico, com acionamento vinte e quatro horas por dia, sete dias por semana, pelo período de 12 (doze) meses;

II - Os acionamentos do suporte técnico serão requisitados por meio de chamados, a serem abertos pelo Contratante por e-mail ou sítio de internet da Contratada/Fabricante;

III - Não haverá limitação no número de chamados que poderão ser abertos durante o período de vigência das subscrições;

IV - A Contratada manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

a) Número sequencial da ordem;

b) Data e hora de abertura;

c) Severidade;

d) Descrição do problema;

e) Data e hora do início do atendimento;

f) Data e hora de término do atendimento.

V - O atendimento em regra será de forma remota. Em caso de impossibilidade do atendimento remoto, o mesmo será realizado de forma presencial;

VI - O suporte técnico deverá ser prestado por profissional com conhecimento nas soluções tecnológicas aplicadas na prestação dos serviços contratados;

VII - A Contratada deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para a Contratante;

VIII - Deverá ser garantida durante o prazo de vigência do contrato a atualização de versões, releases, componentes (bibliotecas, filtros, dentre outros) e módulos dos softwares que compõem a solução ofertada;

IX - O suporte técnico ficará submetido ao Acordo de Níveis de Serviços presente neste documento.

7.7. **Necessidades Tecnológicas**

As especificações técnicas do objeto bem como a descrição dos serviços que compõem a solução foram descritas no Anexo I deste Termo de Referência.

8. **LEVANTAMENTO DAS ALTERNATIVAS DE MERCADO**

8.1. Desde já, há que se salientar que, diferentemente de outras soluções propostas, verifica-se que ainda não existem rankings nacionais ou internacionais de líderes do mercado em soluções de *compliance* em LGPD, visto que tal solução é voltada ao atendimento específico da legislação brasileira, e por este motivo, não se pode contar, por exemplo, com as análises do *Gartner,* da NSS *Labs* ou qualquer outra referência internacional.

8.2. Existem no mercado brasileiro várias empresas que fornecem soluções de *software* para adequação a LGPD. Todavia, verifica-se que os fabricantes de tais soluções não possuem ainda um padrão para o fornecimento desse tipo de *software*, pois enquanto alguns fabricantes fornecem as *feature*s da solução licenciadas de maneira individual, outros vendedores trabalham com uma suíte de funcionalidades, agrupadas em um ou poucos licenciamentos distintos.

8.3. Foram consultados diferentes fornecedores de solução de *software* e a conclusão a que se chega é de que o mercado é plenamente capaz de atender aos requisitos do objeto proposto.

8.4. Saliente-se que as subscrições de software previstas nesta solução são oferecidas pelo mercado somente na modalidade SaaS (Software as a Service), não sendo possível a contratação das mesmas por aquisição perpétua.

8.5. Considerando os requisitos básicos e os padrões acima especificados, visualizam-se no mercado de TIC as seguintes soluções capazes de atender a essa demanda:

8.5.1. **Solução 1: Execução direta pelo órgão**

I - **Vantagem:**

a) Baixo custo teórico em relação a outras alternativas que envolvam técnicos externos, uma vez que a equipe já se encontra alocada no órgão.

II - **Desvantagens:**

a) Impossibilidade de formação de uma equipe técnica com nível de conhecimento equivalente ao do apoio de um técnico analista em LGPD, em virtude da dificuldade de capacitação e da necessidade dos nossos analistas atuarem em diferentes tecnologias, o que não permite a especialização;

b) Número reduzido de servidores para alcançar na velocidade planejada (180 dias);

c) Ausência, no inventário de ferramentas tecnológicas desta autarquia, de soluções para atender às necessidades levantadas no estudo preliminar e não há tempo para o desenvolvimento, visto que a necessidade é premente. Há necessidade de equipe dedicada para atuar nas questões de privacidade de dados e que envolvam pedidos e incidentes com titulares ou seus dados.

8.5.2. **Solução 2: Contratação de empresa para prestação de serviço de consultoria e apoio na adequação Lei Geral de Proteção de Dados Pessoais**

I - **Vantagens:**

a) Os serviços de consultoria darão um panorama completo de informações para adequação à Lei n° 13.709/2018, permitindo que esse trabalho venha a ser desenvolvido em parte ou em sua plenitude por servidores.

b) A contratação de empresa permitirá que as atividades sejam executadas no menor tempo possível, possibilitando que o órgão seja adequado à Lei n° 13.709/2018 em menor tempo.

c) Por meio da contratação, poderão ser demandados entre outros, serviços para treinamento e repasse de conhecimento aos servidores dos órgãos, possibilitando capacitá- los nos temas de privacidade e proteção de dados pessoais para operarem um programa de privacidade e governança dos órgãos.

d) A contratação eventual de serviço de consultoria será capaz de auxiliar os órgãos na elaboração da documentação e implantação das etapas de adequação a LGPD (diagnóstico, governança LGPD, configuração, integração e sustentação).

II - **Desvantagens:**

a) Grande parte dos órgãos não possuem ferramentas tecnológicas para atender às necessidades levantadas no estudo preliminar, sendo necessário realizar todo trabalho de forma manual, podendo demandar um grande volume de profissionais, o que demonstra baixa eficiência.

b) A ausência de tecnologias para implementar um programa de privacidade deixará o órgão contratante exposto pela não conformidade com a Lei n° 13.709/2018.

c) Ainda que os prazos obriguem que sejam empregadas tecnologias por parte da empresa Contratada para realizar as atividades de levantamento, a ausência de ferramentas para a manutenção de estratégias de privacidade poderá resultar na não observância de necessidades e fragilidades, resultando em incidentes de segurança e vazamento pela não conformidade ou baixo nível de maturidade.

d) Ao final dos serviços, restaria um grande volume de atividades a serem executadas, cabendo ao órgão contratante desenvolvê-las sem que haja qualquer garantia que estará apta a desenvolver, gerando riscos às suas atividades em virtude da não conformidade com a Lei.

8.5.3. **Solução 3: Contratação de empresa para o fornecimento de subscrição de software de apoio na adequação às obrigações da LGPD**

I - **Vantagens:**

a) A utilização de um software que apoie a contratante em sua adequação à LGPD representa um ganho operacional considerável, pois possibilitará a automatização de diversas tarefas relacionadas ao objetivo da contratação.

II - **Desvantagens:**

a) Caso não seja oferecido nenhum tipo de serviço de consultoria associado à solução de software, haveria a possibilidade da contratante subutilizar o software licenciado, havendo ainda o risco da adequação à LGPD não se concretizar, pois em diversos cenários, a contratante necessitará de um suporte de consultoria em LGPD para que os objetivos sejam alcançados.

8.5.4. **Solução 4: Contratação de empresa para o fornecimento de subscrição de software de apoio na adequação às obrigações da LGPD, bem como o fornecimento eventual de serviços relacionados ao objeto**

I - **Vantagens:**

a) A oferta de serviços por empresa dotada de recursos técnicos para o apoio nos trabalhos de mapeamento, adequação e compliance dão grande chance de sucesso ao projeto e permitirão que o órgão contratante esteja adequado à LGPD no menor tempo possível.

b) A execução dos serviços combinadas ao fornecimento de tecnologias permitirá que todas as informações levantadas sejam inseridas nos softwares que passarão imediatamente a suportar os processos de tratamento de dados.

c) A execução de diagnósticos de segurança de forma recorrente reforçará medidas de segurança em menor tempo e dará maior eficiência, demonstrando, perante a Autoridade Nacional de Proteção de Dados - ANPD, que o órgão contratante está implementando todas as medidas técnicas viáveis para evitar a exposição ou vazamento de dados de titulares.

d) Uma vez contratado o software em adição ao serviço de consultoria e apoio, a empresa contratada poderia ser responsabilizada por qualquer omissão, negligência em suas estratégias de privacidade e proteção dos dados pessoais ou falha no projeto de compliance, reduzindo os impactos ao órgão contratante.

e) Uma vez implementado um programa de privacidade e proteção dos dados, suportado pelas tecnologias, o órgão contratante terá maior independência de empresas para manutenção do programa, reduzindo os custos de mão de obra terceirizada ao longo do tempo e internalizando gradativamente as atividades de operação das tecnologias e manutenção das informações.

II - **Desvantagens:**

a) A implementação de software em conjunto com os serviços de mapeamento e adequação possuem um valor de investimento alto, ainda que necessário.

b) O projeto possui várias entregas e demandará equipe por parte dos órgãos para execução e acompanhamento das atividades e validação das mesmas.

9. AVALIAÇÃO COMPARATIVA

9.1. Diante da ausência de referências comparativas relevantes entre as diferentes soluções de adequação LGPD disponíveis no mercado brasileiro, foi desenvolvido um quadro comparativo próprio, onde constam cinco *softwares*, de fabricantes distintos, para adequação à LGPD, observados no mercado.

9.2. Houve uma dificuldade inicial em se estabelecer comparativos dos parâmetros técnicos entre os diferentes fabricantes, considerando os diversos resultados encontrados na pesquisa realizada, pois cada qual apresenta via de regra, características técnicas/funcionais semelhantes, ainda que oferecidas em diferentes formatos e pacotes, apresentando inclusive diferentes métricas de quantidade. Destarte, optou-se por incluir na tabela aquelas soluções que compartilhavam características técnicas comuns entre si. O resultado da pesquisa é visto no quadro a seguir:

Benchmark Solução LGPD					
CARACTERÍSTICAS	**Fabricantes**				
	Trust Arc	**One Trust**	**Security**	**Secure Privacy**	**LGPD Now**
Mapeamento de Dados	SIM	SIM	SIM	SEM INFO	SIM
Descoberta e Classificação de Dados	SIM	SIM	SIM	SEM INFO	SIM
Direitos dos Titulares	SIM	SIM	SIM	SEM INFO	SIM
Gestão de Riscos	SIM	SIM	SIM	SIM	SIM
Treinamento e Conscientização	SIM	SIM	SIM	SEM INFO	SIM
Gestão de Atendimento a Titulares, Denúncias e Governança de Certificados	SIM	SIM	SIM	SIM	SIM
Gestão de Incidentes	SIM	SIM	SIM	SEM INFO	SIM
Gerenciamento de Cookies	SIM	SIM	SIM	SIM	SIM
Gestão de Consentimentos	SIM	SIM	SIM	SIM	SIM
Gestão de Políticas	SIM	SIM	SIM	SIM	SIM

10. ANÁLISE DE PROJETOS SIMILARES

10.1. Não há contratações similares feitas pelo PRODERJ.

10.2. No caso em tela, foram realizadas pesquisas no intuito de identificar projetos similares, conforme se infere do estudo preliminar realizado. As pesquisas foram realizadas no Painel de Preços do Ministério da Fazenda.

10.3. Abaixo segue resumo da pesquisa realizada conforme Estudo Técnico:

TABELA COMPARATIVA DE CONTRATAÇÕES SIMILARES					
ÓRGÃO	**INDEXADOR SEI**	**PREGÃO ELETRÔNICO Nº**	**LEI**	**DEFINIÇÃO DO OBJETO**	**VALOR DE REFERÊNCIA (R$)**
Banco do Estado do Espírito Santo	31687479	050/2021	13.303/2016	Licenciamento de software de gestão, para gerenciar o cumprimento às obrigações legais perante a Lei Geral de Proteção de Dados Pessoais -LGPD, com prestação de serviços de Implantação e Integração, Treinamento, Consultoria Operacional e Serviços Adicionais.	sigiloso (previsão legal)
Centrais Elétricas do Norte do Brasil S.A – Eletronorte	31687249	17086/2019	13.303/2016	Contratação de consultoria para adequação da Eletronorte à Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).	-//-
Companhia de Água e Esgoto do Ceará – CAGECE	31687488	20200079	13.303/2016	Serviço de consultoria para adequação da CAGECE à Lei Federal nº 13.709/2018 –Lei Geral de Proteção de Dados Pessoais (LGPD)	-//-
Companhia de Águas de Joinville	40542654	7425620/2020	13.303/2016	Consultoria para diagnóstico de segurança cibernética e aderência à Lei Geral de Proteção de Dados	-//-
Companhia de Saneamento Municipal de Juiz de Fora - CESAMA- MG	40542783	023/2021	13.303/2016	Contratação de consultoria para adequação da CESAMA à Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), envolvendo: o diagnóstico de impacto da LGPD na CESAMA, elaboração do plano estratégico de implementação de um programa de conformidade com a LGPD e implantação do plano estratégico de conformidade com a LGPD.	95.000,00 (oferta vencedora: Shield Segurança da Informação e Consultoria Empresarial Ltda)
Conselho Federal de Contabilidade	31687511	006/2021	8.666/1993	Contratação de serviços de consultoria técnica para conscientização, diagnóstico preparatório e auxílio às atividades de conformidade à Lei 13.709/2018 -Lei Geral de Proteção de Dados Pessoais (LGPD)	514.228,69 (valor médio estimado no edital)
Conselho Federal de Química	40542074	007/2021	8.666/1993	Contratação de empresa para prestação de serviços de consultoria no levantamento e mapeamento de processos e sistemas que tratam dados pessoais visando à construção de programa de conformidade à lei Geral de Proteção de Dados – LGPD, contemplando o monitoramento do plano de ação, uma vez que deverá haver cronograma de execução para a implantação da LGPD por todos os entes do Sistema CFQ/CRQs.	109.333,34 (valor médio estimado no edital)
Conselho Nacional de Justiça	31687513	002/2022	8.666/1993	Contratação de empresa especializada na prestação de serviços e soluções para adequação do CNJ à Lei 13.709/2018, Lei Geral de Proteção de Dados (LGPD).	2.117.359,14 (valor de referência no edital)
Conselho Regional de Fisioterapia e Terapia Ocupacional da 7ª Região - CREFITO 7	40543097	002/2021	8.666/1993	Contratação de pessoa jurídica para desenvolvimento e assessoria para implementação de programa de adequação à Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, de 14 de agosto de 2018e demais alterações, no âmbito do Conselho Regional de Fisioterapia e Terapia Ocupacional da Sétima Região – CREFITO 7,	46.034,67 (valor de referência no edital)

				conforme especificações e condições estabelecidas neste Edital e seus anexos.	
Conselho Regional de Medicina – MG	31687265	004/2021	8.666/1993	Contratação de empresa especializada para implantar no Conselho Regional de Medicina do Estado de Minas Gerais a conformidade com a LGPD como serviço, em consonância com as especificações constantes neste documento.	-//-
Ministério Público do Estado do Acre	40543488	019/2021 (SRP)	8.666/1993	Contratação de serviços de implantação de programa de governança e gestão em privacidade e proteção de dados (em observância ao capítulo VII na seção II da LGPD que trata das Boas Práticas e da Governança), incluindo garantia de atualizações, implantação e suporte técnico pelo prazo de 12 (doze) meses.	238.164,00 (oferta vencedora: Itware Soluções em Tecnologia da Informática Ltda / Contrato nº 067/2021)
SEBRAE-SP	31692029	034/2021	-------	Contratação de empresa especializada em serviço de operação e monitoramento da solução de segurança da informação do SISTEMA SEBRAE, compreendendo serviço de gestão de vulnerabilidades, serviço de monitoramento de ataques cibernéticos, serviço de respostas aos incidentes de segurança e de privacidade, serviço de operações e respostas às requisições, serviço de governança, risco e conformidade de segurança e privacidade em ti, serviço de continuidade de negócio, serviço de testes de invasão, serviço de criptografia de disco, serviço de prevenção contra vazamento de informações em endpoints, serviço de controle de acesso à rede, serviço de descoberta e mapeamento de dados pessoais e sensíveis, serviço de gestão de consentimento e cookies, serviço de distribuição inteligente de fluxo de aplicações e segurança de aplicações web, serviço de anonimização e proteção de dados, serviço de inteligência aplicado à segurança e serviços técnicos especializados, por 36 (trinta e seis) meses.	149.915,00 (menor lance apresentado, renegociado BSG Serviços e Soluções EIRELI- EPP)
Tribunal de Contas do Estado de São Paulo	40543612	012/2021	8.666/1993	Contratação de consultoria especializada para adequação à Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)	59.506,78 (valor de referência no edital)

10.4. Ressalte-se que, conforme informações obtidas através do estudo realizado pelos setores responsáveis pelo planejamento da contratação, não existem soluções de software livre ou *software* público, capazes de satisfazer plenamente os requisitos definidos.

11. JUSTIFICATIVA DA SOLUÇÃO DE TIC ESCOLHIDA

11.0.1. Diante das possíveis opções para alcançar o objetivo pretendido na presente contratação e avaliando a falta de maturidade dos órgãos sobre o tema, a Opção 1 que prevê a execução direta pelo órgão é tecnicamente inviável.

11.0.2. A Opção 2 é tecnicamente viável, entretanto demandará um volume grande de profissionais para operacionalizar as atividades necessárias a um programa de privacidade e proteção de dados, que provavelmente resultará em maiores custos e poderá acarretar riscos de atraso na execução pela ausência do emprego da tecnologia, podendo ser inclusive, economicamente inviável.

11.0.3. A Opção 3 é tecnicamente viável, mas não ofereceria nenhum tipo de apoio externo ao projeto de adequação, o que seria temerário em diversos cenários. Nesta opção, o contratante poderia contar apenas com os treinamentos na solução de software, o que poderia não ser suficiente para a adequação LGPD como um todo. Esta opção exigiria um alto grau de maturidade do órgão contratante acerca das rotinas e etapas para o enquadramento das exigências da LGPD.

11.0.4. A Opção 4 propõe a subscrição do software com o apoio externo, implementando o software para automatizar atividades que são humanamente impossíveis de serem executadas com alto grau de precisão bem como levariam muito tempo para serem concluídas, e apoio externo para serviços agregados que irão apoiar no diagnóstico e adequação à LGPD, implementando medidas e estruturando um programa de privacidade, no software.

11.0.5. Dado o contexto, entende-se que a Opção 4 seria a mais adequada a este contexto, já que o componente de software desempenhará um papel fundamental na manutenção da conformidade legal a ser obtida, contando ainda com o auxílio dos eventuais serviços de consultoria técnica em LGPD.

11.0.6. O objeto é proposto em lote único para melhor se ajustar ao contrato do Sistema de Registro de Preços, bem como ao nível de maturidade na adequação de cada órgão contratante. Contudo, há que se resguardar que a adjudicação do conjunto de itens venha de um mesmo fabricante, uma vez que se trata de solução única, cujos itens resguardam interdependência técnica entre si.

11.0.7. Veja-se quadro comparativo:

	Software	Serviços e Consultorias
OPÇÃO 1	NÃO	NÃO
OPÇÃO 2	NÃO	SIM
OPÇÃO 3	SIM	NÃO
OPÇÃO 4	SIM	SIM

12. JUSTIFICATIVA DO PARCELAMENTO DA SOLUÇÃO

12.1. O objeto ora pretendido se configura em uma solução de TIC composta por mais de um item, os quais têm suas funcionalidades unificadas e administradas em conjunto. Logo, a contratação dos itens da solução de LGPD, bem como a execução dos serviços agregados na forma identificada, garante não só o melhor cumprimento dos requisitos técnicos e tecnológicos, mas também uma melhor unicidade técnica para a entrega das funcionalidades requisitadas pelo PRODERJ.

12.2. O agrupamento dos itens correspondentes à solução de LGPD justifica-se por conta da diversidade dos ambientes tecnológicos nos órgãos da Administração Pública Estadual, levando em conta a quantidade de bancos e bases de dados que aquele órgão possua. Esta escolha estratégica foi tomada no sentido de evitar sub/hiper dimensionamentos aos órgãos participantes, uma vez ventilada a conveniência de licitação da presente solução proposta, via Sistema de Registro de Preços.

12.3. Ademais, o agrupamento dos itens permite uma gestão mais eficiente do ambiente de TI, não apenas no âmbito da funcionalidade da solução, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, a resolução de conflitos entre fornecedores distintos. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado, não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, o suporte técnico, e os treinamentos serão executados por um único fornecedor representante do fabricante. Dessa forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores.

12.4. Assim, entende-se que é fundamental para a pretensa contratação e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que todos os itens ora propostos sejam contratados de forma agrupada.

12.5. Na situação em apreço, é imperativo destacar o que dispõe o Princípio da Padronização, insculpido no inciso I do art. 15 da Lei nº 8.666/1993, pelo qual se estabelece que a Administração, sempre que possível, tem o objetivo de compatibilizar especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia, segundo transcrição a seguir, *in verbis*:

> "Lei nº 8.666/1993 Art. 15. As compras, sempre que possível, deverão:
>
> I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;
>
> (...);
>
> III - submeter-se às condições de aquisição e pagamento semelhantes às do setor privado."

12.6. Tal princípio visa a propiciar à Administração uma consecução mais econômica e vantajosa de seus fins, e serve, pois, como instrumento de racionalização da atividade administrativa, por meio da redução de custos financeiros, tecnológicos, operacionais, gerenciais, técnico-administrativos e da otimização da aplicação de recursos. Isto é, fatores que se coadunam e se verificam na contratação ora pretendida. Significa, portanto, que, nesse caso, a padronização elimina variações tanto no tocante à seleção de componentes e produtos no momento da contratação, como também na sua utilização, conservação, segurança e manutenção.

12.7. Dividir o conteúdo do lote entre fabricantes distintos, ocasionará prejuízos técnicos, como também riscos de danos tecnológicos, visto que a instalação, o suporte técnico e os treinamentos, se realizados por vários fornecedores, exigiriam um tempo excessivo em dirimir divergências entre possíveis incompatibilidades e causariam um potencial risco de operacionalização e funcionamento, pela adoção de procedimentos variados ou divergentes.

12.8. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes das soluções, melhor gerenciamento do contrato e obtenção dos serviços de suporte e treinamentos padronizados.

12.9. Conforme Acórdão nº 861/2013 - TCU - Plenário - é lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Tal entendimento corrobora com a solução de TI, objeto da contratação em tela, que sugere essa indivisibilidade em razão da natureza dos itens que a compõem.

12.10. Segundo o Acórdão nº 5.260/2011 – TCU – 1ª câmara, de 06/07/2011, *"Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si".*

12.11. O lote proposto pelo corpo técnico do PRODERJ agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à competitividade.

12.12. O agrupamento também encontra amparo na jurisprudência do Tribunal de Contas da União, conforme se observa na Súmula 247 - TCU/2007. *"É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade*." (grifos nossos).

12.13. Em suma, a opção pelo fornecimento por lote leva em conta a modalidade de contratação pretendida e os benefícios associados. Tal agrupamento não compromete a competitividade do certame, uma vez que várias empresas, que atuam no mercado, apresentam condições para cotar os itens pretendidos para futura contratação, conforme manifestações do corpo técnico responsável pelo planejamento.

12.14. Na tabela a seguir, segue resumo das justificativas para cada item que compõe o objeto a ser licitado:

SOLUÇÃO LGPD - LOTE			
ITEM	**DESCRIÇÃO**	**MÉTRICA**	**JUSTIFICATIVA**
1	Subscrição de solução de gestão para adequação e governança de conformidade com a LGPD, incluindo suporte técnico e atualização de software pelo período de 12 meses	unidade	É o principal componente de software do objeto. O item compreende todas as funcionalidades da ferramenta. Uma licença cobre toda uma instituição por 1 ano e poderá ser complementado com a contratação dos itens 2 a 4.
2	Subscrição de solução de descoberta e mapeamento de dados estruturados e não estruturados, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade	Este item corresponde a quantidade de bancos de dados a serem tratados, onde uma unidade corresponde a uma instância de banco de dados ou fonte de dado não-estruturado.
3	Subscrição de solução para conscientização e treinamento em segurança e privacidade, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade	Este item corresponde a quantidade de usuários da contratante.
4	Subscrição de solução de Gestão de Atendimento a Titulares, Denúncias e Governança de Certificados em conformidade com a LGPD, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade	Este item corresponde a quantidade de usuários da solução que atuarão na administração e nos processos de atendimento implementados na solução.
5	Treinamento na Solução de Gestão LGPD	aluno	Este item corresponde na quantidade de alunos que virá a ser capacitada na solução, independentemente da quantidade de turmas que vierem a ser ministradas.
6	Serviço de consultoria para apoio na implementação das soluções e adequação à LGPD	UST	Este item corresponde a contratação de serviços de consultoria, por demanda, para auxílio na implementação das soluções e na realização de diagnóstico e adequação à LGPD bem como no apoio ao Encarregado (DPO) e na operação, configuração, integração e sustentação da Solução e estratégias para manutenção da conformidade com a LGPD, onde os serviços serão demandados por meio da emissão de Ordem de Serviço utilizando como métrica para precificação dos serviços a quantidade de UST necessária, baseada em catálogo de serviços.

12.15. O lote, composto dos itens 1, 2, 3, 4, 5 e 6, deverá ser adjudicado para um único fornecedor, uma vez que as atividades desempenhadas para a consecução da Solução formam um conjunto indissociável, composto pela interligação dos serviços, que funcionam harmonicamente.

12.16. O PRODERJ opta por agrupar os serviços distintos no lote, para fins de licitação, uma vez que as melhores práticas de gestão em TIC se baseiam na integração desses serviços, que apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

12.17. É importante também se observar o posicionamento do Egrégio Tribunal de Contas da União, que assim se manifestou sobre o tema:

> "*Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, verbis: "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes..." (grifos não constam do original).*
>
> *Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.*
>
> *Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: "O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória." (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209)."*

12.18. Pode-se afirmar ser tecnicamente inadequado o seu desmembramento além do proposto, sob pena de não atender ao objetivo buscado pelo PRODERJ.

12.19. **Justificativas das Métricas Adotadas no Objeto**

12.19.1. Considerando as nuances da solução e a possível oferta do objeto no contexto de Sistema de Registro de Preços, o presente estudo utilizou métricas variadas para possibilitar a correta precificação dos itens que compõem o lote . Seguem abaixo as justificativas das métricas:

a) Item 1 do objeto - "Subscrição eventual de solução de gestão para adequação e governança de conformidade com a LGPD, incluindo suporte técnico e atualização de software pelo período de 12 meses": Para este item, que será o principal componente de software da solução, dentre os modelos de software disponíveis, opta-se pelo mais simples, que não exige grande conhecimento prévio sobre os ambientes das contratantes. Nesta linha de raciocínio, o formato subscrição anual "por organização", mostra-se plenamente compatível com as necessidades do objeto proposto.

b) Item 2 do objeto - "Subscrição eventual de solução de descoberta e mapeamento de dados estruturados e não estruturados, incluindo suporte técnico e atualização do software pelo período de 12 meses": Ainda que se tenha optado pela simplicidade, tentando reduzir ao máximo os itens correspondentes a solução de software, um aspecto comum nas soluções dos fabricantes consultados é que todas elas levam em conta a quantidade de bancos de dados e fontes de dados não-estruturados que a contratante possui. Deste modo, foi necessário adaptar a solução de software para eventual Sistema de Registro de Preços, e para esta finalidade foi criado este item, cuja unidade se dará pela quantidade de "instâncias de bancos de dados" ou "fontes de dados não-estruturados" da contratante.

c) Item 3 do objeto - "Subscrição de solução para conscientização e treinamento em segurança e privacidade, incluindo suporte técnico e atualização do software pelo período de 12 meses": Ainda que pautado pela simplicidade, visando maior competitividade, o componente de conscientização e treinamento em segurança e privacidade foi desmembrado em virtude do licenciamento baseado na quantidade de usuários da contratante.

d) Item 4 do Objeto – "Subscrição de solução para Gestão Integrada de Chamados e Incidentes em conformidade com a LGPD, incluindo suporte técnico e atualização do software pelo período de 12 meses" que por se tratar de componente importante mais não essencial, a depender da complexidade da Contratante, foi desmembrado para que fosse possível sua contratação apenas por aqueles que necessitem de processos automatizados integrados com demais plataformas de atendimento da organização, tendo como unidade a "quantidade de usuários" que atuaram nos atendimentos pela plataforma.

e) Item 5 do objeto - "Contratação eventual de Treinamento na Solução de Gestão LGPD: Neste item, foi utilizada a métrica "unidade/aluno" em vez de "unidade/turma", de modo que os órgãos solicitem e paguem apenas pela quantidade de alunos que necessitem, no momento que for mais conveniente, dentro do período de duração da Ata. Caso se optasse pela modalidade "unidade/turma", ter-se-ia que estipular a quantidade de alunos desta turma, abrindo assim a possibilidade de os órgãos contratarem treinamento para uma quantidade de pessoas que talvez não corresponda a suas demandas. A ementa dos treinamentos será definida em comum acordo entre contratante e contratada, onde caso a contratante não realize a aquisição de todos os componentes, o tempo previstos para os outros componentes poderá ser utilizado para maior detalhamento do funcionamento dos recursos contratados bem como a realização de exercícios práticos "hands on".

f) Item 6 do objeto – "Contratação eventual de serviço de consultoria para apoio na implantação das soluções e adequação à LGPD": O quantitativo UST a ser contratado vai depender do nível de maturidade e conhecimento do contratante e deverão ser verificados na etapa de Plano de Suprimentos - PLS/SIGA-RJ. Ao consultar alguns fornecedores da solução pretendida, pôde-se averiguar que é comum a cobrança em UST para prestação desse tipo de serviço, sendo possível determinar a quantidade de UST a partir da indicação, a partir de um catálogo de serviços, das atividades e quantidades que serão executadas.

12.20. **Considerações sobre o uso da medição em UST (Unidade de Serviço Técnico) para o item 6 (serviços de consultoria)**

12.20.1. A utilização da métrica por UST, para medição do item 6 que define a solução ora proposta à licitação, que compreende os serviços de consultoria em LGPD, levou em consideração a própria lógica de tais serviços, caracterizados por resultados medidos conforme especificações previamente estabelecidas em um Catálogo de Serviços detalhado.

12.20.2. Unidade de Serviço Técnico é uma métrica para a medição do esforço na execução de um serviço que envolva atividade humana não mensurável previamente com precisão, sendo certo que qualquer técnica com precisão de mensuração que seja inferior a 90%, é candidata a ser substituída pela UST. É bastante utilizada em contratos de prestação de serviços que envolvam diversos tipos de serviços com variados graus de especificidade.

12.20.3. Saliente-se que tal opção, neste certame, está em conformidade com as orientações do Egrégio Tribunal do Contas da União sobre o tema constantes no *Acórdão nº 2037/2019-TCU. Plenário. TC014.760/2018.*

13. **DESCRIÇÃO DA SOLUÇÃO COMO UM TODO**

Contratação de empresa para o fornecimento de solução tecnológica de apoio na adequação às obrigações da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.

14. **DA LICITAÇÃO**

14.1. **Natureza do Objeto da Contratação**

As atividades que integram o objeto da contratação possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste Termo de Referência. Portanto, se enquadram como SERVIÇOS COMUNS ou usuais de mercado, conforme prevê o Parágrafo único do artigo 1º da Lei 10.520/ 2002.

14.2. **Sistema de Registro de Preços**

14.2.1. Considerando as características do serviço que se pretende contratar e que os benefícios a serem alcançados com a presente contratação poderão beneficiar de forma significativa as demandas represadas dos órgãos da Administração Pública para adequação à LGPD, visando evitar a prestação descentralizada desse serviço, o que aumentaria significativamente seus custos, propõe-se a adoção do Sistema de Registro de Preços.

14.2.2. Além disso, as características do serviço, a potencial possibilidade de contratações frequentes e a impossibilidade de se estimar o quantitativo da demanda são argumentos que justificam a adoção da lógica do Sistema do Registro de Preços, entendimento que se extrai das disposições do art. 15, II da Lei nº 8.666/1993.

14.2.3. Em âmbito Estadual o tema é regulamentado pelo Decreto Estadual nº 46.751/2019. Nos termos do art. 3° do normativo referido "o Registro de Preços para a contratação de bens e serviços relativos a tecnologia da informação caberá ao Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro (PRODERJ), na qualidade de Órgão Gerenciador , conforme estabelecido pelo Decreto n° 46.665/2019."

14.2.4. Os serviços objeto do Registro de Preços poderão ser adquiridos pelo Órgão Gerenciador e pelos Órgãos e entidades da Administração Pública direta, autárquica e fundacional do Estado do Rio de Janeiro, ora denominados Órgãos Participantes.

14.2.5. A Ata de Registro de Preços poderá ser aderida por quaisquer órgãos ou entidades do Estado, que não tenham participado do certame licitatório, ora denominados Órgãos Aderentes.

14.2.6. Podem também ser considerados **ÓRGÃOS ADERENTES** os órgãos ou entidades municipais, distritais, de outros estados e federais, resguardadas as disposições de cada ente.

14.2.7. O ÓRGÃO ADERENTE poderá, mediante prévia anuência do ÓRGÃO GERENCIADOR, aderir à Ata de Registro de Preços, desde que realizado estudo que demonstre a viabilidade e a economicidade.

14.2.8. O quantitativo decorrente da contratação pelos Órgãos Aderentes não ultrapassará, na totalidade, ao dobro de cada item da ata de registro de preços e nem poderá exceder, por Órgão Aderente, a cinquenta por cento do quantitativo de cada item desta licitação, registrados na Ata de Registro de Preços para o Órgão Gerenciador e Órgãos Participantes.

14.2.9. O prazo de validade da Ata de Registro de Preços não será superior a 12 (doze) meses.

14.2.10. A Ata de Registro de Preços poderá ser aderida durante a sua vigência por órgãos ou entidades do Estado que não tenham participado do certame licitatório, mediante anuência do PRODERJ, desde que realizado estudo que demonstre a viabilidade da economicidade.

15. **MODALIDADE DE LICITAÇÃO**

15.1. **Pregão Eletrônico**

15.1.1. O objeto da contratação foi conceituado pelo setor técnico responsável pelo planejamento da contratação nos Estudos Preliminares como *"serviço de natureza comum"* que segundo a legislação de regência são "*identificados como aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, mediante as especificações usuais do mercado*" (art. 1º, parágrafo único, da Lei nº 10.520/2002), vale dizer, *bens de aquisição rotineira e habitual, cujas características encontrem no mercado padrões usuais de especificação, envolvendo critérios de julgamento rigorosamente objetivos, não havendo óbices a adoção do Pregão na modalidade eletrônica.*

15.1.2. Desta forma, a modalidade de licitação mais adequada é o PREGÃO, nos termos do art. 1°, parágrafo único da Lei n° 10.520/2002 , sem nenhuma restrição de realização por MEIO ELETRÔNICO.

15.2. **Forma de Adjudicação**

A forma de adjudicação será pelo **MENOR PREÇO GLOBAL POR LOTE.**

16. **JULGAMENTO DAS PROPOSTAS E CRITÉRIO DE ACEITAÇÃO DE PREÇOS**

16.1. O critério de julgamento visará o menor preço ofertado pelo lote.

16.2. A proposta de preços deverá ser feita em moeda nacional e englobará todas as despesas relativas ao objeto do contrato, bem como os respectivos custos diretos e indiretos, tributos, remunerações, despesas fiscais e financeiras e quaisquer outras necessárias ao cumprimento do objeto da Licitação, salvo expressa previsão legal. Nenhuma reivindicação adicional de pagamento de preços será considerada.

16.3. Demais considerações serão definidas em Edital.

17. **CRITÉRIOS DE HABILITAÇÃO**

17.1. **Requisitos de Qualificação Técnica-Operacional**

17.1.1. Para fins de comprovação de qualificação técnica, deverão ser apresentados Atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem a experiência e aptidão de desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, referente às subscrições de software similares às pretendidas, na forma do artigo 30, § 4º, da Lei Federal nº 8.666/93 que indiquem nome, função, endereço de contato do(s) atestador(es), ou qualquer outro meio para eventual contato pelo órgão licitante.

17.1.2. Os atestados deverão comprovar experiência no fornecimento, instalação e configuração de soluções tecnológicas de gestão de LGPD, bem como comprovar a experiência na prestação de serviços técnicos contemplando as seguintes atividades: Diagnóstico e mapeamento de dados, gestão de riscos à privacidade, gestão de consentimentos e preferências, gestão de requisições dos titulares e violações de dados, conscientização em segurança e privacidade, análise de segurança, análise de conformidade com normas e frameworks de segurança e Apoio ao Encarregado (DPO).

17.1.3. Um único atestado é suficiente para a demonstração da experiência anterior do licitante em relação a execução do objeto licitado, sendo possível o somatório de atestados de períodos concomitantes para comprovar a sua capacidade técnica.

17.1.4. A experiência prévia exigida se justifica em razão da necessidade da empresa vencedora demonstrar que detém capacidade para executar simultaneamente os serviços, atendendo satisfatoriamente os quantitativos, em tempo hábil e atendendo ao volume e níveis de serviços.

17.1.5. Os critérios de qualificação técnica, observado o caráter modular da solução e as razões para o modelo de adjudicação do objeto em lote composto por itens interdependentes, bem como a condição inédita desta solução tecnológica no âmbito desta Administração, buscam resguardar os entendimentos assentados pelo Egrégio TCE-RJ no seu processo nº 104.338-3/17, VOTO GA-3 de 21/09/2017.

17.2. **Qualificação Profissional da Equipe da Contratada**

17.2.1. Visando agregar maior qualidade e segurança à contratação, a empresa classificada em primeiro lugar deverá dispor de composição mínima de equipe técnica necessária para a execução dos serviços, conforme abaixo se relaciona:

CARGO	ATRIBUIÇÕES	EXPERIÊNCIA	CERTIFICAÇÕES
Ao menos 1 Gerente de Projeto	Responsável pela gestão do projeto, isso envolve a gestão da equipe e dos recursos de uma maneira geral, o desenvolvimento dos planos de projeto, a comunicação para todos os envolvidos, acompanhamento e divulgação do status e a verificação e validação dos pacotes de trabalho, conforme cronograma proposto e demais atividades contempladas no escopo do projeto.	Profissional com curso superior, preferencialmente, em Tecnologia da Informação ou área relacionada ao objeto. Comprovação da experiência de pelo menos 1 (um) ano, atuando como gerente de projetos, em empresa pública ou privada. A comprovação se dará através da apresentação e análise dos currículos e evidências da experiência, tais como declarações e atestados de capacidade técnica cujo nome do profissional esteja relacionado.	Certificação PMP (Project Management Professional) ou PRINCE 2 ou Pós-graduação em Gestão de Projetos. Essas certificações se referem à competência do profissional para a gestão de projetos e liderança de equipes de trabalho, sendo desejável em rezão das características da contratação pretendida, que envolverá atividades voltadas à proteção de dados pessoais sensíveis. São certificações reconhecidas em mais de 150 países e definem que o profissional está capacitado em um alto padrão de qualidade para a gestão de projetos, seguindo padrões ISO (International Organization for Standardization). O sistema ISO de qualidade tem por função promover a normatização de produtos e serviços, cuja qualidade está em aprimoramento permanentemente. Saliente-se que a Associação Brasileira de Normas Técnicas (ABNT) é o órgão responsável pela normalização técnica no Brasil e também é representante do sistema ISO.
Ao menos 1 Especialista em Privacidade de Dados	Responsável pela coordenação das atividades do projeto, que envolve o diagnóstico detalhado, avaliação, mapeamento dos processos que temos tratamento de dados, documentação dos processos, mapeamentos dos principais riscos à privacidade e elaboração do relatório de impacto e demais atividades contempladas no escopo do projeto.	Profissional com curso superior em Tecnologia da Informação ou Direito. Comprovação da experiência de pelo menos 1 (um) ano, atuando em privacidade de dados, atuando em projetos de diagnóstico e adequação à LGPD. A comprovação se dará através da apresentação e análise dos currículos e evidências da experiência, tais como declarações e atestados de capacidade técnica cujo nome do profissional esteja relacionado.	Certificação EXIN Certified Data Protection Officer ou IAPP Certified Information Privacy Manager. A certificação DPO é um atestado de que o profissional possui o conhecimento e as competências necessárias para ser Encarregado de Dados pessoais dentro de uma estrutura corporativa. Dentre as certificações atuais observadas no mercado, a EXIN e a IAPP são as de maior destaque e reconhecimento. São desejáveis aos profissionais que prestarão a consultoria de apoio ao DPO do órgão contratante, como garantia de qualidade, em razão da novidade que a proteção de dados representa no âmbito da administração pública, onde não se dispõe amplamente de quadros preparados para os desafios que a atividade demanda.
Ao menos 1 Especialista em Mapeamento de Dados	Responsável pelo mapeamento dos fluxos do cenário de tratamento de dados, identificação dos GAPs, recomendações e ações, documentação dos processos, procedimentos e atividades levantados e demais atividades contempladas no escopo do projeto.	Profissional com curso superior, preferencialmente, em Tecnologia da Informação. Comprovação da experiência de pelo menos 1 (um) ano, atuando no mapeamento de dados em projetos de adequação à LGPD. A comprovação se dará através da apresentação e análise dos currículos e evidências da experiência, tais como declarações e atestados de capacidade técnica cujo nome do profissional esteja relacionado.	Certificação Information Security Foundation based on ISO IEC 27001 e Certificação EXIN Certified Data Protection Officer ou IAPP Certified Information Privacy Manager. A certificação ISO 27001 é o padrão internacional para a gestão da Segurança da Informação, escopo principal do serviço ora proposto à contratação. A certificação DPO é um atestado de que o profissional possui o conhecimento e as competências necessárias para ser Encarregado de Dados pessoais dentro de uma estrutura corporativa. Dentre as certificações atuais observadas no mercado, a EXIN e a IAPP são as de maior destaque e reconhecimento. São desejáveis aos profissionais que prestarão a consultoria de apoio ao DPO do órgão contratante, como garantia de qualidade, em razão da novidade que a proteção de dados representa no âmbito da administração pública, onde não se

			dispõe amplamente de quadros preparados para os desafios que a atividade demanda.
Ao menos 1 Especialista / Analista Jurídico	Responsável pelas análises técnicas em contratos e das bases legais para cada finalidade, papéis e responsabilidades do encarregado e demais atividades contempladas no escopo do projeto.	Profissional com curso superior em Direito e registro na OAB Comprovação da experiência de pelo menos 1 (um) ano, atuando em projetos de adequação à LGPD e de apoio ao Encarregado (DPO). A comprovação se dará através da apresentação e análise dos currículos e evidências da experiência, tais como declarações e atestados de capacidade técnica cujo nome do profissional esteja relacionado.	Certificação EXIN Certified Data Protection Officer ou IAPP Certified Information Privacy Manager. A certificação DPO é um atestado de que o profissional possui o conhecimento e as competências necessárias para ser Encarregado de Dados pessoais dentro de uma estrutura corporativa. Dentre as certificações atuais observadas no mercado, a EXIN e a IAPP são as de maior destaque e reconhecimento. São desejáveis aos profissionais que prestarão a consultoria de apoio ao DPO do órgão contratante, como garantia de qualidade, em razão da novidade que a proteção de dados representa no âmbito da administração pública, onde não se dispõe amplamente de quadros preparados para os desafios que a atividade demanda.
Ao menos 1 Especialista em Segurança da Informação	Responsável por identificar e classificar ativos de informação, analisar vulnerabilidades, conduzir análise e avaliação dos riscos, avaliar e propor processos para resposta a incidentes, garantindo a confidencialidade e a integridade dos dados.	Profissional com curso superior em Tecnologia da Informação ou área relacionada ao objeto. Comprovação da experiência de pelo menos 2 (dois) anos, atuando como profissional nas áreas de tecnologia e conhecimento no estabelecimento de boas práticas em segurança e privacidade e gestão de riscos. A comprovação se dará através da apresentação e análise dos currículos e evidências da experiência, tais como declarações e atestados de capacidade técnica cujo nome do profissional esteja relacionado.	Certificação Information Security Foundation based on ISO IEC 27001 A certificação ISO 27001 é o padrão internacional para a gestão da Segurança da Informação, escopo principal do serviço ora proposto à contratação.

17.2.2. Admite-se vínculo entre os profissionais e a empresa Contratante através de contrato de trabalho, contrato de prestação de serviços ou através de vínculo ao quadro societário.

17.2.3. A comprovação de atendimento a este requisito de habilitação poderá ser feita mediante a apresentação de declaração formal de disponibilidade, exigível após a adjudicação, para a execução do contrato, tal como prescreve o §6° do art. 30 da Lei 8.666/93, se sujeitando a contratante as sanções legais em caso de descumprimento contratual.

17.2.4. No momento da assinatura do contrato deverão ser apresentados currículos e cópias de diplomas dos integrantes que compõem a equipe técnica da contratada.

17.2.5. **Justificativas para a exigência das certificações dos profissionais a atuarem na prestação do serviço de apoio na adequação às obrigações da Lei nº 13.709/2018.**

17.2.5.1. Tanto o PRODERJ quanto os demais órgãos participantes dependem dos produtos e serviços em questão para realizarem as adequações necessárias para conformidade com a Lei nº 13.709/2018. A exigência que a empresa que vier a ser contratada detenha minimamente um profissional para cada perfil necessário a execução do objeto tem por objetivo evitar atraso ou má qualidade na prestação dos serviços.

17.2.5.2. Somado a isso e tendo em vista que, trata-se de uma lei nova cujos agentes públicos ainda estão buscando capacitação e treinamento para lidarem com os desafios relacionados a sua implementação, o emprego de mão de obra com qualificação técnica, conhecimento e experiência prática mitiga o risco de, ao final da prestação dos serviços, os resultados esperados não tenham sido alcançados.

17.2.5.3. Ademais, a Lei 8.666/93, na etapa de habilitação, ressalta a necessidade de a Administração analisar a qualificação técnica dos licitantes, com o objetivo de aferir se dispõem de conhecimento, experiência e aparelhamento técnico e humano suficiente para satisfazer o contrato celebrado.

17.2.5.4. Dito isso, revela-se indispensável que o edital preveja certificações que garantam o bom desempenho e andamento do serviço a ser licitado, não adentrando o caso na seara de restrição da ampla concorrência, vez que em consonância com Constituição Federal, em seu artigo 37, inciso XXI, não se trata de exigência excessiva, além de ser justificada e proporcional ao serviço a ser executado.

> "*Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:[...]*
>
> *XXI - ressalvados os casos especificados na legislação, as obras, serviços, compras e alienações serão contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes, com cláusulas que estabeleçam obrigações de pagamento, mantidas as condições efetivas da proposta, nos termos da lei, o qual somente* ***permitirá as exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações****." **(grifo nosso)***

17.2.5.5. Nesse sentido, com base em diversas contratações recentes com o objetivo de adequar as empresas e órgãos onde essas contratações ocorreram, o PRODERJ optou por qualificar minimamente os perfis de equipe que entende como necessários para qualificar a empresa que virá a ser contratada para a prestação dos serviços.

17.2.5.6. Além dos editais referenciados pelo corpo técnico no estudo , foram identificados outros editais mais recentes cujas contratações da mesma forma buscaram qualificar minimamente os profissionais que viriam a ser engajados na execução do objeto, das quais damos destaque aos Editais da Companhia de Águas e Esgoto do Estado do Rio de Janeiro (CEDAE) e da Empresa Brasileira de Petróleo (PETROBRÁS) cujo objeto guarda enorme similaridade com a contratação em questão, onde foram solicitados como requisitos mínimos de qualificação, comprovação de que a licitante detém, previamente a formalização do Contrato, equipe com qualificações mínimas que vão muito além daqueles que estão sendo solicitados neste Termo de Referência, senão vejamos:

REQUISITOS DE PROFISSIONAIS - PETROBRÁS Licitação: Oportunidade nº 7003863393 (junho/2022)				
Perfil	**Formação**	**Experiência**	**Proficiência em inglês**	**Certificações profissionais**
Gerente	Formação superior	No mínimo 5 anos de experiência profissional em consultoria; Experiência em, no mínimo, 3 projetos de adequação à LGPD e/ou GDPR;	Leitura, escrita e conversação	Obrigatória pelo menos uma certificação de cada grupo listado abaixo: **Certificação PMP do PMI; Grupo Privacidade: Exin:** Privacy and Data Protection Foundation (PDPF) ou Privacy and Data Protection Practitioner (PDPP); **Maastricht University:** DPO Certification; **IAPP:** CIPM, ou CIPP; **Grupo Segurança / Riscos:** ISACA: CISM, CISA ou CRISC; ISO 27001 ou 27002. ISC2: CISSP.
Profissionais com Perfil 1	Formação superior	No mínimo 5 anos de experiência profissional em consultoria; Experiência em, no mínimo, 3 projetos de adequação à LGPD e/ou GDPR;	Leitura, escrita e conversação	Obrigatória pelo menos uma certificação de cada grupo listado abaixo: **Grupo Privacidade: Exin:** Privacy and Data Protection Foundation (PDPF) ou Privacy and Data Protection Practitioner (PDPP); **Maastricht University:** DPO Certification; **IAPP:** CIPM ou CIPP; **Grupo Segurança / Riscos:** ISACA: CISM, CISA ou CRISC; ISO 27001 ou 27002.

				ISC2: CISSP.
Profissionais com Perfil 2	Formação superior	No mínimo 2 anos de experiência em privacidade e de dados pessoais com experiência em avaliação de riscos	Leitura, escrita	Obrigatória pelo menos uma certificação: **Grupo Privacidade:** **Exin:** Privacy and Data Protection Essentials based on LGPD(PDPE) ou Privacy and Data Protection Foundation (PDPF) ou Privacy and Data Protection Practitioner (PDPP); **Maastricht University:** DPO Certification; **IAPP:** CIPM, CIPP ou CIPT;

REQUISITOS DE PROFISSIONAIS - CEDAE Pregão Eletrônico nº 639/2021		
Cargo	**Atribuição**	**Experiência / Certificação**
Gerente de Projeto	Responsável pela gestão do projeto, isso envolve a gestão da equipe e dos recursos de uma maneira geral, o desenvolvimento dos planos de projeto, a comunicação para todos os envolvidos, acompanhamento e divulgação do status e a verificação e validação dos pacotes de trabalho, conforme cronograma proposto.	Profissional com curso superior, preferencialmente, em Tecnologia da Informação ou Administração. Certificação PMP (Project Management Professional), ou PRINCE 2. Comprovação da experiência de pelo menos 1 (um) ano, atuando como gerente de projetos, em empresa pública ou privada com no mínimo 1.000 (mil) funcionários. A comprovação se dará através da apresentação e análise dos currículos.
Especialista em Segurança da Informação	Responsável por identificar vulnerabilidades em servidores, aplicações e sistemas, conduzir avaliação sobre a disponibilidade dos recursos, análise de riscos, resposta a incidentes e controle de acesso, garantindo a confidencialidade e a integridade dos dados da Companhia.	Profissional com curso superior em Tecnologia da Informação. Certificação ISO/IEC 27001 (Padrão para Sistema de Gestão da Segurança da Informação); e, Certificação ITIL 4 Foundation ou Certificação COBIT 5 Foundation. Comprovação da experiência de pelo menos 1 (um) ano, atuando como profissional de segurança da informação e conhecimento em práticas de proteção de dados. Ter realizado avaliação de segurança da informação, gestão de vulnerabilidades, gestão de riscos e gestão de incidentes.
Especialista em Privacidade de Dados	Responsável pela coordenação das atividades do projeto, que envolve o diagnóstico detalhado, avaliação, mapeamento dos processos que temos tratamento de dados, documentação dos processos, relatório de impacto, e demais atividades contempladas no escopo do projeto.	Profissional com curso superior, preferencialmente, em Tecnologia da Informação ou Direito. Certificação EXIN Privacy and Data Protection Practitioner; ou, EXIN Certified Data Protection Officer; ou, IAPP Certified Information Privacy Manager. Comprovação da experiência de pelo menos 1 (um) ano, atuando como especialista em privacidade de dados, realizando o diagnóstico detalhado, análise de riscos, mapeamento de processos, relatório de impacto, em empresa pública ou privada. A comprovação se dará através da apresentação e análise dos currículos.
Especialista em Mapeamento de Processos	Responsável pelo mapeamento dos fluxos do cenário de privacidade de dados (Marketing, RH, Comercial, Segurança da Informação, Jurídico, Ouvidoria Geral), mapeamentos dos principais riscos, identificação dos GAPs, recomendações e ações, documentação dos processos, procedimentos e atividades levantados.	Profissional com curso superior, preferencialmente, em Tecnologia da Informação. Certificação ISO/IEC 27001 (Padrão para Sistema de Gestão da Segurança da Informação); e, Certificação ITIL 4 Foundation ou Certificação COBIT 5 Foundation. Comprovação da experiência de pelo menos 1 (um) ano, atuando no mapeamento de processos em projetos de adequação à LGPD. A comprovação se dará através da apresentação e análise dos currículos.
Especialista / Analista Jurídico	Responsável pela análise dos contratos e das bases legais para cada finalidade, papéis e responsabilidades do Controlador e do Operador.	Profissional com curso superior em Direito e registro na OAB. Certificação EXIN Privacy and DataProtection Practitioner; ou EXIN Certified Data Protection Officer; ou IAPP Certified Information Privacy Manager. Comprovação da experiência de pelo menos 1 (um) ano, atuando em projetos de adequação à LGPD. A comprovação se dará através da apresentação e análise dos currículos.

17.2.5.7. Tais exigências visam trazer maiores garantias em relação aos resultados dos serviços que virão a ser contratados e encontram amparo no que preconiza o Acórdão nº 1214/2013-TCU-Plenário:

> "*Para que se obtenha a proposta mais vantajosa é necessária a especificação do produto ou* ***serviço adequada às reais necessidades da Administração e a formulação de exigências de qualificação técnica*** *e econômico-financeira* ***que não restrinjam a competição e propiciem a obtenção de preços compatíveis com os de mercado, mas que afastem empresas desqualificadas do certame****." **(Grifo nosso)***

17.2.5.8. Ainda em relação ao acórdão supracitado e proferido pelo relator Aroldo Cedraz, foi fiel a legislação ao mencionar que:

> "***9. Nessa linha de raciocínio, é essencial que a Administração reexamine seus editais, inserindo critérios rigorosos de habilitação, em especial no que se refere às qualificações técnico-operacional, profissional, e econômico-financeira das licitantes.***
>
> *80. Cumpre observar que o art. 3º da Lei 8.666/93 fixa orientação no sentido de* ***que "A licitação destina-se a garantir a observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional, e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos****". 134. Quanto à qualificação técnico-profissional, pretende-se a uniformização da interpretação do art. 30, § 1º, inciso I, parte final, da Lei nº 8.666/1993, que prevê vedação de exigências de quantidades mínimas ou prazos máximos nos atestados utilizados para a comprovação da capacidade técnico-profissional das empresas licitantes.*
>
> *135. Eis a redação do dispositivo objeto da controvérsia interpretativa:*
>
> "*Art. 30. A documentação relativa à qualificação técnica limitar-se-á a: (...)*
>
> *§ 1º A comprovação de aptidão referida no inciso II do "caput" deste artigo, no caso das licitações pertinentes a obras e serviços, será feita por atestados fornecidos por pessoas jurídicas de direito público ou privado, devidamente registrados nas entidades profissionais competentes, limitadas as exigências a: (Redação dada pela Lei nº 8.883, de 1994)*
>
> *I – capacitação técnico-profissional: comprovação do licitante de possuir em seu quadro permanente, na data prevista para entrega da proposta, profissional de nível superior ou outro devidamente reconhecido pela entidade competente, detentor de atestado de responsabilidade técnica por execução de obra ou serviço de características semelhantes, limitadas estas exclusivamente às parcelas de maior relevância e valor significativo do objeto da licitação, vedadas as exigências de quantidades mínimas ou prazos máximos;" (Incluído pela Lei nº 8.883, de 1994).*
>
> *[...]*
>
> *136. Destaque-se que, para a contratação de serviços de natureza continuada,* ***a necessidade de exigências técnico-profissionais estará relacionada à complexidade técnica envolvida em sua execução.*** *A título de exemplo, podemos citar serviços nos quais historicamente são realizadas exigências dessa natureza: manutenção predial, ar-condicionado, serviços de engenharia em geral, áudio e vídeo, informática.* ***(Grifo Nosso)."***

17.2.5.9. A corroborar com a afirmação ora defendida, seguem precedentes do Colendo STJ:

> "*RECURSO ESPECIAL – ADMINISTRATIVO – LICITAÇÃO PÚBLICA – SERVIÇOS DE LIMPEZA E CONSERVAÇÃO – EDITAL – ART. 30, II, DA LEI nº 8.666/93 – EXIGÊNCIA DE CAPACITAÇÃO TÉCNICA E FINANCEIRA LÍCITA – ART. 57, II, DA LEI nº 8.666/93 – AUSÊNCIA DE PREQUESTIONAMENTO – PRESTAÇÃO DE SERVIÇOS DE FORMA CONTÍNUA – PATRIMÔNIO LÍQUIDO MÍNIMO – DURAÇÃO DO CONTRATO FIXADA AB INITIO EM 60 MESES – ILEGALIDADE – RECURSO ESPECIAL PROVIDO EM PARTE.*
>
> ***É certo que não pode a Administração, em nenhuma hipótese, fazer exigências que frustrem o caráter competitivo do certame, mas sim garantir ampla participação na disputa licitatória, possibilitando o maior número possível de concorrentes, desde que tenham qualificação técnica e econômica para garantir o cumprimento das obrigações.***
>
> ***Dessarte, inexiste violação ao princípio da igualdade entre as partes se os requisitos do edital, quanto à capacidade técnica, são compatíveis com o objeto da concorrência.***
>
> *(...)". Recurso especial provido em parte. (REsp 474.781/DF, Rel. Ministro FRANCIULLI NETTO, SEGUNDA TURMA, julgado em 08/04/2003, DJ 12/05/2003 p. 297)* ***(Grifo Nosso)***

> "*ADMINISTRATIVO. LICITAÇÃO. EDITAL. HABILITAÇÃO. QUALIFICAÇÃO TÉCNICA DO LICITANTE. EXIGÊNCIA LEGAL. REGISTRO OU INSCRIÇÃO NA ENTIDADE PROFISSIONAL COMPETENTE. PRECEDENTES. RECURSO PREJUDICADO.*
>
> *I – A habilitação do particular, antes denominada capacidade jurídica, é a aptidão efetiva do interessado, seja ele pessoa física ou jurídica, para exercer direitos e contrair obrigações, com responsabilidade absoluta ou relativa por seus atos, ligando-se visceralmente à pessoa partícipe do certame da licitação, e não às qualidades de seus funcionários.*
>
> *II – O art. 30, inc. I, da Lei nº 8.666/1993, ao regular a habilitação dos interessados, dispõe que a qualificação técnica se limita à apresentação de registro ou inscrição na entidade profissional competente. Contempla-se, assim, a comprovação da aptidão da pessoa do licitante em cumprir com todas as obrigações atinentes à execução do objeto da licitação.*
>
> ***III – A qualificação técnica do particular licitante é pressuposto indispensável ao adimplemento de sua habilitação no certame público, uma vez que a Administração somente poderá confiar-lhe a execução do objeto da licitação, se o interessado possuir e comprovar, nos termos da lei (art. 30, inc. I, da Lei nº 8.666/1993), a sua habilitação jurídica plena. Precedentes do STJ.***
>
> *IV – Dado ao lapso de tempo transcorrido desde o ajuizamento do mandamus, vê-se que os serviços, objeto da licitação questionada, já foram realizados, tornando o recurso prejudicado pela perda do seu objeto". (RMS 10.736/BA, Rel. Ministra LAURITA VAZ, SEGUNDA TURMA, julgado em 26/03/2002, DJ 29/04/2002 p. 209)."* ***(Grifo Nosso)***

17.2.5.10. Desse modo, revela-se pertinente e adequado e não ofende os princípios licitatórios da competitividade, isonomia e legalidade, é prudente e justificada a inserção no Edital de exigências relacionadas à exigência de certificação para avaliação quanto a capacidade técnico-profissional dos licitantes.

17.2.5.11. Por fim, tendo em vista que o papel a ser desempenhado pelo profissional na função de Especialista / Analista Jurídico do projeto é a realização de análises técnicas em contratos e das bases legais para cada finalidade, papéis e responsabilidades do encarregado de dados (DPO), entende-se como fundamental que este profissional minimamente possua formação superior em Direito, preferencialmente com registro na OAB.

17.2.5.12. Tal entendimento é praxe em contratações dessa natureza, como demonstrado nas contratações já citadas no Estudo Técnico, das quais como referência citamos a Companhia de Água e Esgoto do Ceará - CAGECE que no Pregão Eletrônico nº 202000079 solicita no item 4.1.6.1. *"equipe que deverá ser certificada, no mínimo, em Privacy & Data Protection Essentials, composta por profissionais cujo perfil mais sênior será o de pesquisa técnica e jurídica,* ***sendo advogados com expertise em direito digital****, compliance e privacidade profissionais técnicos (ciência de dados, analytics e data mapping)"*; a Companhia de Saneamento Municipal - CESAMA que no Pregão Eletrônico nº 23/2021 solicitou no item 5.2 do Termo de Referência, entre outros Consultor Jurídico "*Responsável pela coordenação da análise dos contratos firmados pela CESAMA e orientações com base na LGPD com* ***Diploma de formação superior em Direito e registro na OAB***", além da Companhia de Água e Esgoto do Estado do Rio de Janeiro – CEDAE que no Edital de Pregão Eletrônico nº 639/2021, da mesma forma prevê profissional com os mesmos requisitos de formação solicitados nesta contratação.

18. CRITÉRIOS DE ACEITAÇÃO DO OBJETO

18.1. Teste de Bancada

18.1.1. Concluída a etapa de lances do pregão e resguardado o período de envio de documentos, será exigido teste de bancada do licitante classificado em primeiro lugar.

18.1.2. O Teste de Bancada tem por objetivo a comprovação de que a solução ofertada pelo licitante arrematante é compatível com as exigências técnicas necessárias e prescritas para este objeto.

18.1.3. O licitante arrematante será convocado, no prazo máximo de até 72 (setenta e duas) horas para reunião (virtual), onde serão definidas as tratativas para definição do ambiente de teste.

18.1.4. Nesta reunião o licitante deverá entregar os documentos oficiais da(s) Solução(ões) que permitam comprovar o atendimento aos requisitos técnicos constantes do Anexo I deste documento, sob pena de desclassificação no caso do não envio da documentação dos produtos, necessária para avaliar se os produtos ofertados possuem os recursos necessários ao atendimento dos requisitos técnicos especificados, apresentando no mínimo:

a) ID do requisito;

b) Descrição do requisito;

c) Nome do produto ofertado;

d) Nome do documento de referência onde é possível verificar evidência do atendimento do requisito;

e) Página do documento referência onde é possível verificar evidência do atendimento do requisito;

f) Outras informações necessárias.

18.1.5. O teste poderá ser realizado no ambiente do PRODERJ, nos endereços abaixo mencionados, a ser acertado em reunião:

a) Data Center – Centro Integrado de Comando e Controle (CICC). End.: Rua Carmo Neto s/nº, Cidade Nova, Rio de Janeiro – RJ - CEP 20210-051; ou

b) Sede – Centro de Tecnologia da Informação e Comunicação do Governo do Estado do Rio de Janeiro (PRODERJ) . End.: R. da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011.

18.1.6. Se optar por realizar o teste no ambiente do PRODERJ, o arrematante deverá informar todos os requisitos necessários para a instalação do ambiente de teste.

18.1.7. O LICITANTE deverá disponibilizar ao menos 01 (um) técnico que se responsabilizará pela instalação do software da solução, caso o teste seja realizado utilizando a infraestrutura do PRODERJ.

18.1.8. A disponibilização dos hardwares e softwares necessários à realização do teste de bancada são de inteira responsabilidade da proponente, onde será fornecido computador com acesso à internet e equipamento para projeção.

18.1.9. Admite-se, alternativamente, o uso de ambiente virtual do fabricante ou da licitante arrematante para comprovação das funcionalidades da solução ofertada, conforme acordado em reunião.

18.1.10. Em caso de não comparecimento à reunião (por problema único e exclusivo do LICITANTE) o teste de bancada acontecerá no ambiente padrão de teste do PRODERJ, em um dos endereços acima citados, sendo vedado ao LICITANTE arrematante reivindicar qualquer adaptação na infraestrutura oferecida.

18.1.11. O PRODERJ, por meio da Comissão Permanente de Licitação (Pregoeiro), dará publicidade, através do chat de mensagens do SIGA-RJ, da data de realização do teste que deverá ocorrer no prazo de 5 dias após a realização da reunião.

18.1.12. Se o teste for realizado em ambiente do PRODERJ, o LICITANTE terá até as 17h do dia anterior ao da realização do mesmo para providenciar a instalação do ambiente nas condições definidas na reunião.

18.1.13. O prazo de 5 dias, do subtópico 18.1.11, poderá ser prorrogado por igual período, mediante requisição fundamentada do LICITANTE, mantida a mesma regra de limite para a instalação do ambiente.

18.1.14. O teste de bancada será realizado entre 10:00 e 18:00 horas (horário de Brasília).

18.1.15. Os custos para realização do teste de bancada são de responsabilidade do LICITANTE e em hipótese alguma caberá qualquer tipo de indenização.

18.1.16. Os demais licitantes que tenham participado da etapa competitiva e desejem acompanhar a sessão, poderão indicar um representante para acompanhamento, devendo para tanto enviar para o e-mail da Comissão Permanente de Licitação (cdl@proderj.rj.gov.br) até as 16hs do dia que antecede a sessão de teste. No e-mail deverão constar: dados da empresa interessada (nome e contato), de seu representante (nome e contato) para o devido credenciamento.

18.1.17. No dia de realização do teste, o licitante que será avaliado, bem como os demais interessados em acompanhar, deverão chegar ao local indicado com antecedência mínima de 30 minutos.

18.1.18. Na sessão de teste de bancada, a equipe técnica do PRODERJ considerará apto o sistema que atender os requisitos conforme descrito no Anexo III - Roteiro para Teste de Bancada, deste Termo de Referência, onde cada item deverá ser preenchido, observados os critérios "atende" ou "não atende".

18.1.19. Ao término do teste de bancada será emitido um atestado de demonstração, que atestará se o(s) software(s) cumpre(m) os requisitos técnicos necessários.

18.1.20. Durante o teste de bancada poderá ser feito questionamento, exclusivamente pelos representantes do PRODERJ à proponente permitindo a verificação dos requisitos estabelecidos.

18.1.21. Ao final do teste de bancada a Comissão Técnica emitirá relatório sucinto descrevendo os testes realizados e a conclusão sobre a aprovação da proposta ou desclassificação.

18.1.22. Para a equipe técnica considerar o sistema apto a ser contratado pela administração, todos os requisitos de software que constam no presente estudo e seu anexo de especificações técnicas, deverão ser considerados ATENDIDOS.

18.1.23. Será desclassificada a licitante que for convocada para o teste de bancada e não demonstrar a compatibilidade de seu produto conforme as especificações técnicas exigidas ou não comparecer no dia marcado sob qualquer pretexto.

18.1.24. Em caso de desclassificação no teste de bancada deverá ser convocada a próxima proponente na ordem de classificação, resguardadas todas as condições e prazos previstos neste tópico.

19. MODELO DE EXECUÇÃO DO CONTRATO

O objeto será executado segundo o regime de execução por empreitada por preço unitário.

19.1. Forma de Execução do Contrato

19.1.1. O fornecedor deve disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.

19.1.2. O fornecedor deverá submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações da Ata.

19.1.3. O fornecedor deverá elaborar um relatório, sobre a prestação dos serviços, a ser entregue à Comissão de Fiscalização do contrato após a entrega do objeto, para a emissão do termo de recebimento provisório.

19.1.4. O relatório deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual. Por fim, o relatório, conforme os respectivos itens de serviço que estejam sendo entregues, deve observar o seguinte:

a) Para os itens 1 a 4: estar acompanhado da documentação que comprove o licenciamento das soluções contratadas, tais como número de séries, chaves, dados para acionamento dos serviços de suporte e documentos oficiais do fabricante e documentação do produto e a disponibilização das soluções.

b) Para o item 5: deve também conter os dados dos alunos, a data de realização do treinamento, o nome do instrutor, a ementa e carga horária executada (mínimo de 40 horas), bem como estar acompanhado dos certificados dos alunos treinados.

c) Para o item 6: estar acompanhado da documentação que comprove a entrega dos produtos e serviços descritos nas Ordens de Serviço, observados os entregáveis respectivamente previstos no Catálogo de Serviços constante do Anexo II deste Termo de Referência.

19.1.5. A instalação e configuração da solução serão executadas conforme a reunião de Kick-off prevista no subtópico 19.4. deste documento.

19.2. Abertura de Chamados

19.2.1. Chamados de suporte técnico e de abertura de serviços serão abertos exclusivamente por meio do sistema de abertura e gerenciamento de chamados provido e mantido pela CONTRATADA sem ônus para o órgão contratante. Cada chamado deverá conter, no mínimo, as seguintes informações:

a) Número de identificação exclusivo;

b) data e hora do início da ocorrência;

c) descrição da ocorrência;

d) nível de severidade;

e) providências adotadas para o diagnóstico;

f) indicação de solução provisória e/ou solução definitiva;

g) data e hora do término da ocorrência, com solução definitiva;

h) identificação do técnico do órgão contratante que solicitou e validou o chamado técnico;

i) identificação do técnico da CONTRATADA responsável pela execução do chamado técnico,

j) outras informações pertinentes.

19.2.2. Deverá existir canal de atendimento para realização e acompanhamento de chamados técnicos, com acesso permanente para os técnicos do órgão contratante, contemplando no mínimo, sítio eletrônico e telefone 0800 (gratuito) ou telefone local no logradouro onde estive sediado o órgão contratante.

19.2.3. O sistema de abertura de chamados deverá estar disponível 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), inclusive feriados.

19.2.4. A CONTRATADA deverá realizar a integração da sua ferramenta de abertura de chamados de modo a permitir o recebimento de alertas e abertura automática de incidentes na ferramenta de IT Service Management (ITSM), ou gestão de serviços de TI (GSTI) do órgão contratante.

19.2.5. Na abertura do chamado técnico, o técnico do órgão contratante definirá um nível de severidade que deverão ser resolvidos, de maneira definitiva, nos prazos estabelecidos de acordo com os níveis de severidade descritos de acordo com o subtópico 23.1.2. deste documento.

19.3. Emissão de Ordem de Serviço – OS

19.3.1. A execução será sempre precedida da emissão de Ordem de Serviço – O.S., contendo no mínimo: descrição do serviço, quantitativo, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço e especificações técnicas do serviço esperados.

19.3.2. A O.S. será emitida, assinada e autorizada pelo Fiscal do Contrato.

19.3.3. Toda O.S. deverá ser assinada pelo Gerente do Projeto ou Preposto, representante da CONTRATADA, declarando a concordância da CONTRATADA em executar as atividades descritas na “Ordem de Serviço – O.S.”, de acordo com as especificações estabelecidas pelo CONTRATANTE.

19.3.4. Antes do fechamento de cada O.S. a CONTRATADA consultará o representante indicado pelo CONTRATANTE, que avaliará e atestará o serviço realizado.

19.4. **Reunião Kick Off**

19.4.1. A CONTRATADA deve realizar, nas dependências do CONTRATANTE, antes do início da implantação da solução, uma reunião de projeto (kick-off) em conjunto com as áreas de Segurança da Informação, de Infraestrutura e com o Encarregado de Dados Pessoais da contratante, para definir o Plano de Trabalho de instalação, configuração e de suporte da solução.

19.4.2. Nesta reunião o Responsável Técnico da Contratada deverá apresentar um cronograma e plano de instalação/configuração dos itens 1 a 4.

19.4.3. A CONTRATANTE deverá disponibilizar máquinas físicas ou virtuais para que as soluções sejam instaladas pela CONTRATADA, caso seja aplicável ou necessário.

19.4.4. Após a reunião de kick-off deve ser produzida uma ata, assinada por todos os participantes da CONTRATADA e da CONTRATANTE, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, da equipe de trabalho, relatório de controle e tratamento da privacidade e demais artefatos que se façam necessários ao atendimento da contratante.

19.4.5. Compreende-se nesta etapa a instalação de sistemas e aplicativos da CONTRATANTE nos PRODUTOS fornecidos, bem como a migração das configurações existentes na CONTRATANTE para os produtos fornecidos pela CONTRATADA, se assim for o caso.

19.4.6. Durante a etapa de instalação e configuração, os produtos fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção.

19.4.7. A CONTRATADA deverá, com a supervisão e aprovação da CONTRATANTE, planejar e realizar a instalação e configuração dos softwares com total interoperabilidade no ambiente atual da CONTRATANTE, sem impacto no ambiente de produção.

19.4.8. Durante a implantação e integração, caso seja necessário, a CONTRATADA deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.

19.4.9. Para instalação e configuração devem ser consideradas as seguintes premissas:

a) Caberá a CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares e recursos humanos necessários à instalação dos PRODUTOS;

b) Caberá a CONTRATADA a disponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da CONTRATANTE caso a instalação dos produtos / softwares da CONTRATADA apresente falha.

c) A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação e ao pleno funcionamento do ambiente de produção.

19.5. **Cronograma**

19.5.1. A entrega dos itens 1 a 6 acontecerá de forma concomitante, pois trata-se da entrega de uma solução de software integrado, bem como a sua instalação e serviços de consultoria. Para que possa ser atestada a entrega dos referidos itens, se fará necessário que:

a) Em até 15 dias após a assinatura do contrato, ocorrerá reunião de kick-off prevista no subtópico 19.4..;

b) Os serviços de treinamento (item 5) deverão iniciar em até 15 (quinze) dias a contar da emissão da Ordem de Serviço.

19.5.2. Os Serviços de consultoria para apoio na implantação das soluções e adequação à LGPD (item 6) serão formalizados por meio da emissão de ordem de serviço onde serão descritos minimamente os dados do demandante, atividades, entregáveis, prazo e a quantidade de UST's correspondentes aos serviços nela especificados.

19.5.3. A data limite para entrega do objeto será sempre contada em dias úteis.

PRAZO	MARCO INICIAL	ATIVIDADE	RESPONSÁVEL
15 dias	publicação do extrato do contrato no Diário Oficial	Reunião de Kick-Off e entrega cronograma e plano de instalação/configuração dos itens de software (itens 1 a 4). Entrega da documentação que comprove o licenciamento das soluções contratadas e disponibilização do acesso a elas.	CONTRATADA e CONTRATANTE
Conforme descrito na O.S. e Cronograma	emissão da O.S.	Implantação das soluções (itens 1 a 4).	CONTRATADA
15 dias	emissão da O.S.	Início do Treinamento (item 5).	CONTRATADA
Conforme descrito na O.S.	emissão da O.S.	Cumprimento dos serviços de consultoria (item 6) demandado, conforme condições e prazos estabelecidos na O.S.	CONTRATADA
24 horas	entrega do objeto	Emissão do Termo de Recebimento Provisório.	CONTRATANTE
20 dias	emissão do termo de recebimento provisório	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura.	CONTRATANTE

19.6. **Forma e Local de Entrega**

19.6.1. A solução tecnológica ora proposta possui os itens 1 a 4 de softwares com entrega virtual (forma remota) na plataforma do contratante.

19.6.2. O item 5 de treinamento com entrega virtual (forma remota) na plataforma do fornecedor/fabricante e o item 6 de serviços de consultoria que poderão ocorrer de forma remota ou presencial.

19.6.3. Há também o suporte técnico agregado aos itens 1 a 4 que também serão prestados, em regra, na modalidade remota, mas com eventuais atendimentos presenciais.

19.6.4. O local de prestação presencial no PRODERJ, quando necessária, será a sua sede localizada na Rua da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011, para as eventualidades em que a prestação do serviço se faça necessária fisicamente.

19.6.5. O local de referência para a prestação presencial, nos demais órgãos participantes foi informada no subtópico 6.7.1. do presente termo de referência.

20. **DO SIGILO, CONFIDENCIALIDADE E SEGURANÇA DOS DADOS E INFORMAÇÕES ACESSADAS**

A CONTRATADA deverá assinar um termo de confidencialidade e sigilo, na forma do modelo do anexo V deste Termo de Referência, a ser anexado ao contrato principal.

21. **NECESSIDADE DE ADEQUAÇÃO DO AMBIENTE**

Não há providências a serem previamente realizadas pelo órgão contratante para viabilizar a celebração do contrato.

22. **FISCALIZAÇÃO DO CONTRATO**

A execução do contrato será acompanhada e fiscalizada por comissão de fiscalização de contrato composta por 3 (três) membros do Contratante, especialmente designados.

22.1. **Mecanismos de comunicação a serem estabelecidos**

22.1.1. São instrumentos formais de comunicação entre a CONTRATANTE e a CONTRATADA:

a) Ordens de Serviço;

b) Plano de Inserção;

c) Termos de Recebimento;

d) Chamado registrado na Central de Atendimento;

e) Ofícios;

f) Relatórios e Atas de Reunião;

g) E-mail;

h) Demais Termos previstos no instrumento convocatório.

22.1.2. A comunicação entre a CONTRATANTE e a CONTRATADA, para fins de encaminhamento de Ordens de Serviço ou outro documento, ocorrerá sempre via por intermédio do preposto, ou seu substituto, designado pela CONTRATADA.

22.1.3. A comunicação dos usuários com a Central de Atendimento/Suporte da CONTRATADA poderá ser realizada por meio de abertura de chamado via telefone com registro de protocolo ou utilização de sistema informatizado que permita o registro da demanda.

23. **ACORDO DE NÍVEL DE SERVIÇO**

23.1. Atender os níveis de serviço exigidos:

23.1.1. Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 05 (cinco) dias por semana;

23.1.2. Para efeito dos atendimentos técnicos, a Contratada deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS	
NÍVEL	**DESCRIÇÃO**
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido.

TABELA DE PRAZOS DE ATENDIMENTO				
MODALIDADE	**PRAZOS**	**NÍVEIS DE SEVERIDADE**		
		1	**2**	**3**
TELEFONE, E-MAIL E WEB	INÍCIO DO ATENDIMENTO	4 HORAS	8 HORAS	48 HORAS
	TÉRMINO DO ATENDIMENTO	8 HORAS	16 HORAS	96 HORAS

23.1.3. Para Nível 1, caso o atendimento não seja finalizado até as 20h, o técnico não poderá interrompê-lo, devendo continuar até sua finalização, ou a interrupção do mesmo pelo responsável técnico da Contratante;

23.1.4. Todo o chamado somente será caracterizado como “encerrado” mediante concordância da Contratante;

23.1.5. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da Contratante.

23.1.6. Estão estabelecidos Níveis de Serviço com a finalidade de aferir e avaliar diversos fatores relacionados aos serviços contratados, bem como orientar o pagamento por resultados obtidos, inclusive para fins de eventuais glosas.

23.1.7. Os critérios deste tópico aplicam-se aos seguintes itens:

a) Subscrição de softwares / suporte técnico (itens 1 ao 4);

b) Treinamento (item 5). Nesse caso, a penalização se dará em razão de eventual atraso no início da prestação, a contar da emissão da Ordem de Serviço;

c) Serviço de consultoria especializada para apoio na adequação à LGPD (item 6). Nesse caso, a penalização se dará por dia de atraso na finalização de uma ordem de serviço, onde a penalização será aplicada no valor correspondente ao(s) produto(s) em atraso;

23.1.8. A contratada deverá cumprir prazos máximos para respostas aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme o quadro do subtópico 23.1.2. deste documento.

23.1.9. O nível de severidade será informado pelo Contratante no momento da abertura do chamado, podendo ser reclassificado a critério do Contratante, caso em que ocorrerá início de nova contagem de prazo para o seu cumprimento.

23.1.10. Ocorrerá aplicação de multa por motivo de descumprimento de nível de serviço exigido, conforme valores a seguir:

a) 0,20% a título de multa a ser descontado na garantia do contrato, por demanda categorizada como "Nivel 3" não atendida no prazo, observados os limites quanto ao início e término do atendimento (para os itens 1 ao 4);

b) 0,50% a título de multa a ser descontado na garantia do contrato, por demanda categorizada como “Nível 2” não atendida no prazo, observados os limites quanto ao início e término do atendimento (para os itens 1 ao 4);

c) 1% a título de multa a ser descontado na garantia do contrato, por demanda categorizada como "Nível 1" não atendida no prazo, observados os limites quanto ao início e término do atendimento, resguardado o quanto diposto no subtópico 23.1.3. (para os itens 1 ao 4);

d) 0,50% no valor da fatura do item correspondente a serviço de treinamento, por dia de atraso após o limite máximo para entrega (para o item 5);

e) 0,10% no valor correspondente ao produto em atraso, por dia de atraso (para o item 6).

23.1.11. As multas por não cumprimento do nível de serviço não serão aplicados para demandas não rotineiras, no caso, por exemplo, de instalação de novas versões de software. Também não serão aplicados se o motivo pelo atraso ou não cumprimento foi causado pela contratante, circunstância que a contratada deverá demonstrar no relatório previsto no subtópico 19.1.3., ficando sujeito à análise e aprovação da Comissão de Fiscalização.

23.1.12. Ficam resguardadas as sanções previstas nos art. 86 a 88, da Lei nº 8.666/1993.

23.1.13. Todas as solicitações de suporte técnico devem ser registradas pela contratada para acompanhamento e controle da execução do serviço;

23.1.14. Para a execução de atendimento, é necessária a autorização do CONTRATANTE para instalação ou desinstalação de quaisquer softwares ou equipamentos que não façam parte da Solução de criptografia da contratada;

23.1.15. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;

23.1.16. Para esses problemas, a contratada deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução paliativa e informar ao CONTRATANTE, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada ao CONTRATANTE;

23.1.17. A contratada deverá, sempre que solicitado, emitir relatórios de atendimento de todas as intervenções realizadas, preventivas ou corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções;

23.1.18. As multas serão descontadas do valor da garantia do contrato, prevista no tópico 30 deste Termo de Referência.

24. **OBRIGAÇÕES DO CONTRATANTE**

a) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

b) Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos;

c) Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;

e) Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

f) Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável; e

h) Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados, pertençam à Administração.

25. **OBRIGAÇÕES DO CONTRATADO**

a) Entregar o objeto conforme as especificações constantes do Termo de Referência e seus anexos;

b) Indicar formalmente preposto apto a representá-lo junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

c) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

d) Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;

e) Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

f) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

g) Manter durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

h) Manter total sigilo e confidencialidade, por si, por seus empregados ou representantes, no que se refere a não divulgação, por qualquer forma ou meio, de toda ou parte de informações ou documentos sobre a Contratante, ou sob guarda da Contratante, bem como toda a informação a respeito dos negócios, ideias, produtos, clientes ou serviços, às quais venha a ter acesso, em decorrência da prestação dos serviços executados;

i) Responsabilizar-se em caso de quebra de sigilo ou mau uso das informações obtidas por seus funcionários ou representantes, em razão da prestação dos serviços;

j) Somente revelar as informações decorrentes da contratação, exclusivamente a seus prepostos e funcionários diretamente envolvidos nas atividades que fazem uso ou tenham acesso permanente ou eventual às mesmas;

k) Respeitar integralmente as normas de segurança estabelecidas pela CONTRATANTE, atendendo os padrões de segurança e controle para acesso e uso das instalações e equipamentos, zelando por sua integridade;

l) Fazer os esforços necessários para garantir que seus empregados e representantes estejam inteiramente cientes dos riscos associados com problemas inerentes à segurança da informação, inclusive quanto a dados pessoais;

m) Disponibilizar previamente as informações necessárias para acesso aos ambientes físico e lógico da CONTRATANTE, para que a mesma analise a liberação dos acessos às dependências, de funcionários, equipamentos, softwares e sistemas que forem necessários ao cumprimento do objeto;

n) Realizar, no fim do contrato, a transição contratual, a saber: a transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações à CONTRATANTE;

o) Arcar com as despesas e responsabilidade pela obtenção das autorizações quanto às eventuais permissões, aprovações e/ou licenças, bem como as respectivas eventuais renovações, junto das autoridades governamentais federais, estaduais e municipais, agentes do serviço público, concessionárias de serviços públicos e quaisquer outros Órgãos/Entidades que se façam necessários à execução do objeto, durante todo o prazo da contratação.

25.1. A CONTRATADA deverá assinar o termo de confidencialidade e sigilo previsto no tópico 20 deste Termo de Referência.

26. **RECEBIMENTO PROVISÓRIO E DEFINITIVO**

26.1. O recebimento provisório será realizado pela equipe de fiscalização, em até 24 horas após a contratada entregar o Relatório de Cumprimento do Objeto indicado no subtópico 19.1.3. deste Termo de Referência, além de:

a) Para os itens 1 a 4: Apresentação da documentação que comprove o licenciamento das soluções contratadas, tais como número de séries, chaves, dados para acionamento dos serviços de suporte e documentos oficiais do fabricante e documentação do produto e a disponibilização das soluções.

b) Para o item 5: Para fins de comprovação da entrega dos serviços, a Contratada deverá produzir, após a realização dos treinamentos, o relatório acima referido deverá conter ao menos os dados dos alunos, a data de realização do treinamento, o nome do instrutor, a ementa e carga horária executada bem como os certificados dos alunos treinados.

c) Para o item 6: Entrega dos produtos e serviços descritos nas Ordens de Serviço, observado o respectivamente previsto no Catálogo de Serviços.

26.2. A contratante analisará a documentação entregue e poderá fazer inspeção quanto às etapas executadas na entrega do objeto, por meio de sua equipe técnica, com a finalidade de verificar a adequação no cumprimento do objeto pela contratada para fins de constatar e relacionar os arremates, retoques e revisões finais que eventualmente se fizerem necessários.

26.3. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não proceder ao recebimento definitivo até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas na fase do recebimento provisório.

26.4. Após o recebimento provisório do objeto, o Gestor do Contrato deverá providenciar em até 20 (vinte) dias o recebimento definitivo, ato que concretiza o ateste do cumprimento do objeto contratado, obedecendo as seguintes diretrizes:

a) Realizar a análise dos relatórios e de toda a documentação apresentada e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à contratada as respectivas correções.

b) Emitir Termo de Recebimento Definitivo do objeto, com base nos relatórios e documentações apresentadas; e

c) Comunicar a empresa para que, no prazo de até 5 (cinco) dias, emita a Nota Fiscal, com o valor exato dimensionado pela fiscalização.

26.5. Em caso de verificação de pendência a ser sanada pela CONTRATADA o prazo para o Recebimento Definitivo ficará suspenso e somente retomado após a devida solução.

27. **PAGAMENTO**

27.1. O pagamento será realizado de modo:

a) A vista, para os itens de subscrição de licença (itens 1, 2, 3 e 4), com suporte técnico agregado, com início após a completa instalação e configuração (entrega definitiva).

b) A vista, sob demanda, para o item de treinamento (item 5).

c) A vista, sob demanda, para o serviço previsto no item 6.

27.2. O pagamento é condicionado à emissão e assinatura do Termo de Recebimento Definitivo pela Comissão de Fiscalização do Contrato.

27.3. O pagamento será realizado no prazo de 30 (trinta) dias, a contar da data final do período de adimplemento.

27.4. Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível ao CONTRATADO, sofrerão a incidência de atualização financeira pelo IBGE/IPCA, e juros moratórios de 0,5% ao mês, calculado *pro rata die,* e aqueles pagos em prazo inferior ao estabelecido neste Edital serão feitos mediante desconto de 0,5% ao mês *pro rata die.*

27.5. A execução financeira do contrato será realizada em parcelas correspondentes às Ordens de Serviço emitidas, conforme a demanda de cada item, ao longo da vigência contratual.

27.6. As demais condições para o pagamento constam no Edital.

28. **VIGÊNCIA CONTRATUAL**

28.1. Prazo de 12 (doze) meses, a contar da publicação do extrato no Diário Oficial.

28.2. O prazo máximo de prorrogação do contrato será de até 48 (quarenta e oito) meses, na forma do art. 57, inciso IV, da Lei nº 8.666/93, observado o Enunciado nº 46 da Douta Procuradoria Geral do Estado do Rio de Janeiro.

28.3. CONTRATADA sujeitar-se-á aos acréscimos e supressões, na forma do art. 65, da Lei. n 8.666/93.

29. **REAJUSTE DE PREÇOS**

29.1. Os valores constantes da Ata de Registro de Preços não sofrerão reajuste, exceto nos casos previstos nos art. 21 e art. 22, do Decreto Estadual nº 46.751/2019, para a renegociação de preços junto aos fornecedores registrados, nos casos em que os preços praticados na Ata de Registro de Preços se tornarem superiores aos preços de mercado, resguardadas as disposições do Edital.

29.2. Os contratos gerados a partir da Ata de Registro de Preços poderão ter os seus preços reajustados, observado o interregno mínimo de 12 (doze) meses contados da data limite da apresentação da proposta pela empresa contratada, aplicando-se a variação do Índice de Preços ao Consumidor Amplo – IPCA, ou outro que o venha substituir, nos termos do art. 40, inciso XI, da Lei nº 8.666/1993.

29.3. O Reajustamento ocorrerá na forma do art. 65, da Lei nº 8.666/93.

30. **GARANTIA CONTRATUAL**

30.1. Exigir-se-á do fornecedor, no prazo máximo de 10 dias, contado da data da assinatura do contrato, comprovante de prestação de garantia da ordem de 5 % (cinco por cento) do valor do contrato, a ser prestada em qualquer modalidade prevista no §1º, do art. 56 da Lei n.º 8.666/93, a ser restituída após sua execução satisfatória.

30.2. O referido percentual, resguardada a discricionariedade prevista no art. 56, caput, da Lei nº 8.666/93 e o teto estabelecido no seu §2º, considera a natureza do objeto, enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do órgão contratante em razão das exigências trazidas pela nova legislação quanto ao tratamento de dados pessoais.

30.3. A garantia, qualquer que seja a modalidade apresentada pelo vencedor do certame, deverá contemplar a cobertura para os seguintes eventos:

a) Prejuízos advindos do não cumprimento do contrato;

b) Multas punitivas aplicadas pela fiscalização à contratada;

c) Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato;

d) Obrigações previdenciárias e trabalhistas não honradas pela Contratada.

30.4. A garantia prestada não poderá se vincular a outras contratações, salvo após sua liberação.

30.5. Caso o valor do contrato seja alterado, de acordo com o art. 65 da Lei Federal n.º 8.666/93, a garantia deverá ser complementada, no prazo de 72 horas, para que seja mantido o percentual de 5 % do valor do Contrato.

30.6. Nos casos em que valores de multa venham a ser descontados da garantia, seu valor original será recomposto no prazo de 72 horas, sob pena de rescisão administrativa do contrato.

31. **CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE**

O fornecedor deverá, no que for aplicável ao cumprimento do objeto, obedecer aos critérios estabelecidos no Decreto Estadual nº 43.629/2012.

32. **POSSIBILIDADE DE SUBCONTRATAÇÃO**

Não se aplica a subcontratação em razão da natureza do objeto, enquanto serviço, em lote, para fornecimento de solução integrada.

O treinamento exercido pelo fabricante não configura subcontratação.

33. **POSSIBILIDADE DE PARTICIPAÇÃO DE CONSÓRCIO**

33.1. Não será permitida a participação de empresas que estiverem reunidas em consórcio, dadas as características específicas da solução a ser contratada, que por sua vez, não pressupõe multiplicidade de atividades empresariais distintas (heterogeneidade de atividades empresariais).

33.2. Tendo em vista que é prerrogativa do Poder Público, na condição de contratante, a escolha da participação, ou não, de empresas constituídas sob a forma de consórcio, conforme se depreende da literalidade do texto da Lei nº 8.666/93, que em seu artigo 33 atribui à Administração a prerrogativa de admissão de consórcios em licitações por ela promovidas, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

33.3. A participação de Consórcio também não será permitida pelos mesmos pontos elencados no tópico 12. *"justificativa do parcelamento da solução"*, tendo em vista que resultaria da mesma forma na prestação dos serviços de forma distribuída entre mais de uma empresa, tornando complexa a gestão por parte da Contratante e oferecendo riscos à privacidade dos dados que serão tratados no decorrer da execução dos serviços.

34. **POSSIBILIDADE DE PARTICIPAÇÃO DE COOPERATIVA**

Diante da especificidade desta contratação, que, além da prestação de serviços técnicos de suporte em tecnologia, agrega o fornecimento de licenças de software os quais englobados em lote, bem como observado o mercado de soluções para o objeto ora proposto, composto por empresas de organização tradicional aptas a fornecer a integralidade do objeto, não se aplica a participação de cooperativas neste certame.

35. **AUDIÊNCIA PÚBLICA**

35.1. Sobre o tema, há orientação da d. PGE, veja-se:

35.2. Enunciado n.º 35 - PGE: Audiência Pública nas licitações

35.3. "Deverá ser realizada audiência pública previamente à licitação quando o valor estimado da contratação, ou do conjunto de licitações simultâneas ou sucessivas, superar 100 (cem) vezes o limite previsto no art. 23, inciso I, alínea c, da Lei nº 8.666, de 1993, nos termos do art. 39, mesmo em se tratando de pregão ou de registro de preços."(Ref.: Parecer nº 76/09-PHDMP, 36/DAMFA/PG-15/2015 e 8/2016-RAT/PG-15, Publicado: DO I, 11 de novembro de 2016 Pág 23 - grifou-se).

35.4. A estimativa do valor da contratação será revelada após a consolidação da pesquisa mercadológica.

36. **SANÇÕES**

O contratado inadimplente estará sujeito às penalidades previstas no art. 87 da Lei Federal nº 8.666/93 e demais penalidades que receberão tratativas no Edital e no Contrato.

37. **ANEXOS**

I - Especificações Técnicas do Objeto (49852091);
II - Catálogo de Serviços UST (49851842);
III - Roteiro para Teste de Bancada (49852217);
IV - Modelo de Ordem de Serviço / Autorização de Compra (49852289);
V - Modelo de Termo de Confidencialidade e Sigilo (49852632);
VI - Modelo de Planilha de Custos (49852700).

38. **ASSINATURA DOS RESPONSÁVEIS PELA ELABORAÇÃO**

Manuelito de Sousa Reis Júnior Gerente de Riscos e Ameaças ID nº 4406953-7	Sâmya Massari Lima Encarregada de Dados Pessoais ID nº 5108516-0

Rio de Janeiro, 22 abril de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/04/2023, às 00:29, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Sâmya Massari Lima**, **Diretora**, em 24/04/2023, às 11:50, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **50738229** e o código CRC **44970714**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Governança e Dados e Informações e

Diretoria de Segurança da Informação

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. SOLUÇÃO DE LGPD - QUADRO DO OBJETO

LOTE	ID SIGA	Descrição	Unidade de Fornecimento	Observação
único	177603	Subscrição de solução de gestão para adequação e governança de conformidade com a LGPD, incluindo suporte técnico e atualização de software pelo período de 12 meses	Unidade	Este item trata da contratação anual do software/solução que dará suporte aos processos necessários ao estabelecimento do programa de privacidade, devendo ser fornecidas licenças para cada órgão que vier a contratar.
	177604	Subscrição de solução de descoberta e mapeamento de dados estruturados e não estruturados, incluindo suporte técnico e atualização do software pelo período de 12 meses	Unidade	Este item trata da contratação anual do software/solução que dará suporte às atividades de descoberta e mapeamento de dados para conformidade com a LGPD.
	177605	Subscrição de solução para conscientização e treinamento em segurança e privacidade, incluindo suporte técnico e atualização do software pelo período de 12 meses	Unidade	Este item trata da disponibilização de recursos para realização de simulações de *phishing* e treinamentos voltados à conscientização de usuários.
	176272	Subscrição de solução de Gestão de Atendimento a Titulares, Denúncias e Governança de Certificados em conformidade com a LGPD, incluindo suporte técnico e atualização do software pelo período de 12 meses	Unidade	Este item trata da contratação anual do software/solução que dará suporte às atividades de gestão dos atendimentos relacionados à LGPD em conformidade com as políticas e a LGPD.
	177644	Treinamento na Solução de Gestão LGPD	Alunos	Este item trata da contratação dos serviços de treinamento.
	177646	Serviço de consultoria para apoio na implementação das soluções e adequação à LGPD	UST	Este item trata da execução, sob demanda, do conjunto de serviços necessários à implantação e operação das soluções, atividades necessárias ao diagnóstico e adequações à LGPD baseado em boas práticas de governança em privacidade, bem como o repasse e apoio assistido ao Encarregado (DPO) e equipes envolvidas na conformidade com a LGPD, conforme catálogo de serviços apresentado neste documento, tendo como referência a quantidade de Unidades de Serviço Técnico –

				UST necessárias a execução de cada uma das atividades que compõe o catálogo.

2. **SOLUÇÃO PARA GESTÃO PARA ADEQUAÇÃO E GOVERNANÇA DE CONFORMIDADE COM A LGPD**

I - A solução deverá ser licenciada para cada órgão que vier a contratá-la, onde cada unidade deverá permitir o cadastramento de até 5 administradores.

II - Os produtos necessários ao atendimento dos requisitos dos componentes da solução deverão ser de um único fabricante ou estarem integrados nativamente sem a necessidade configurações que exijam codificação, exceto no caso de API.

III - Caso venha a ser fornecida em nuvem, a CONTRATADA deverá comprovar que toda a comunicação bem como o ambiente fornecido pelo fabricante é seguro e atende às boas práticas de mercado.

IV - Toda a comunicação com a solução deverá ocorrer utilizando-se de recursos criptográficos, assim como os dados deverão ser armazenados em banco de dados criptografados.

2.1. **REQUISITOS GERAIS**

2.1.1. Todas as funcionalidades da solução que dependam de interação com cliente/usuário devem ser disponibilizadas via interface/aplicação web sem necessidade de instalação de agentes ou conectores nas máquinas dos usuários ou em servidores da CONTRATANTE (Banco de Dados, File Server, etc.).

2.1.2. Não serão aceitas soluções cliente/servidor ou baseadas em software livre.

2.1.3. Não deve haver a necessidade de instalação e nem de utilização de plug-ins nos navegadores para a execução da camada cliente da aplicação web.

2.1.4. As interfaces do usuário, incluindo orientações de uso da solução e todos os manuais, devem estar no idioma inglês ou português.

2.1.5. A aplicação/interface web deve rodar nas versões atuais dos principais navegadores de Internet existentes no mercado à época da instalação da solução e deve garantir compatibilidade com as suas novas versões. Por "principais navegadores de Internet" considere-se, no mínimo, os seguintes: Microsoft Edge, Mozilla Firefox e Google Chrome, independentemente do sistema operacional utilizado (Windows, MAC OS, Linux, etc.).

2.1.6. A solução deverá ser compatível com os navegadores das plataformas de dispositivos móveis: Android e iOS - web adaptativo/responsivo ou possuir aplicativo móvel.

2.1.7. A solução deve permitir a capacidade de se personalizar, no mínimo:

I - Fundos e banners;

II - Menu e ferramentas de navegação;

III - Campos, formulários e tabelas;

IV - Cor do texto, fonte e tamanho;

V - Infográficos, Gráficos e painéis;

VI - Alertas e notificações.

2.1.8. A soluçao deverá possibilitar a auditoria nos processos de adequação à LGPD em cada órgão partícipe do Sistema de Registros de Preços.

2.2. **REQUISITOS DE INTEGRAÇÃO**

2.2.1. A solução deve fornecer mecanismos para integração síncrona e assíncrona com aplicações da CONTRATANTE incluindo RESTful e SOAP APIs, assim como requisições de API GET, PUSH, PULL etc.

2.2.2. A solução deve fornecer integração com serviço de e-mail, devendo ser utilizado servidor SMTP/POP/IMAP provido pela empresa.

2.2.3. A solução deve permitir a integração de sistemas de terceiros e recursos de migração de dados. A solução deve fornecer uma variedade de técnicas de integração, incluindo:

I - Webservices;

II - JDBC;

III - LDAP;

IV - Excel;

V - CSV;

VI - E-mail.

2.2.4. A solução também deve usar tecnologias padrão da indústria, como SOAP, REST ou WSDL. Além disso, as integrações de API e de linha de comando devem ser possíveis usando um MID Server (Middleware/Barramento). Todo o tráfego de Webservices deve ser encriptado com TLS.

2.2.5. A plataforma deve ser baseada em arquitetura orientada a serviços (SOA), na qual todos os objetos de dados podem usar os Webservices para acessar a integração bidirecional de nível de dados.

2.2.6. A plataforma deve oferecer uma interface rica (Rich interface) para carregar dados externos usando conjuntos de importação de várias fonts de dados, como HTTPS, FTPS e SCP usando formatos de arquivo, como XML, CSV e Microsoft Excel XLS.

2.2.7. A solução deve suportar a governança dos dados pessoais de organização hierárquicas, tais como órgãos de um estado ou empresas de um grupo empresarial, permitindo que a gestão dos dados.

2.2.8. A solução deve suportar a governança dos dados pessoais de organizações hierárquicas, (órgãos de um estado), permitindo que a gestão dos dados pessoais destas empresas seja: centralizada, parcialmente distribuída, totalmente distribuída ou variações dessas configurações, de acordo com as necessidades do contratante. Deve atender, no mínimo, aos seguintes cenários:

I - Uma organização central pode gerir todos os dados pessoais das organizações do grupo/órgãos de governo.

II - Cada organização pode administrar os dados pessoais do qual é controladora, porém, a organização central tem visibilidade dos processos comuns e pode ter visibilidade sobre os dados pessoais compartilhados entre as organizações do grupo.

III - Deve ser permitindo que uma ou mais organizações tenham uma gestão dos dados pessoal totalmente independente da organização central.

IV - Que as organizações controladoras, participantes da hierarquia, possam emitir relatórios de consulta sobre a existência de dados pessoais sob sua responsabilidade e que estejam sob custódia de operadores que façam parte da mesma hierarquia.

2.2.9. Por segurança, a solução deverá suportar a instalação dos componentes que necessitam acessar as bases de dados estruturados e não estruturados da CONTRATANTE no datacenter da contratante (*on premises*), em servidores com sistemas operacionais Windows em suas versões mais recentes, ou Linux, nas distribuições mais utilizadas no mercado em suas versões mais recentes. A conexão da plataforma em nuvem com estes servidores de data Discovery, quando for o caso, deverá ser realizada por conexão segura e criptografada.

2.2.10. A CONTRATANTE será responsável por fornecer a infraestrutura de rede, processamento, armazenamento, bancos de dados e licenciamento dos sistemas operacionais utilizados. Todas as demais licenças necessárias ao funcionamento da solução deverão ser fornecidas pela contratada.

2.2.11. A solução deverá possuir portal WEB que permita a avaliação dos itens previstos no PRIVACY BY DESIGN/DEFAULT, sendo:

I - Proativo, e não reativo;

II - Preventivo, e não corretivo;

III - Privacidade como padrão (Privacy by Default);

IV - Privacidade incorporada ao design;

V - Funcionalidade total (soma positiva, não soma-zero);

VI - Segurança de ponta a ponta;

VII - Visibilidade e transparência;

VIII - Respeito pela privacidade do usuário.

2.2.12. A partir da definição da estratégia de dados das áreas de negócio a criação de indicadores que permitam:

I - Medir objetivamente a maturidade das áreas de negócio e TI quanto a disciplinas de gestão de informações;

II - Medir qualidade das informações;

III - Eficiência e eficácia dos processos de governança e gestão dedados;

IV - Engajamento das áreas de negócio e TI.

2.2.13. A solução deverá permitir a criação de painéis gerenciais utilizando técnicas e softwares de B.I. Nativa da própria ferramenta da Contratada para a construção de visões analíticas e gerenciais de todos os módulos previstos na plataforma LGPD. Neste caso, a Contratada ficará com a responsabilidade pelo desenvolvimento, sustentação, construção e apresentação dos dados. Além disso, deverá ser fornecido um painel estratégico, onde serão apresentadas e analisadas as informações de acesso.

2.2.14. Considerando que cada usuário da solução possui necessidades de uma visão gerencial de acordo com suas atividades e processos de trabalho são fundamentais que a solução permita ao próprio usuário da solução, sem apoio técnico e de forma intuitiva, criar seus painéis e dashboards de gerenciamento. Para isso, a solução deverá:

I - Permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte.

II - Permitir a criação de painéis e dashboards com gráficos do tipo pizza, linha, colunas, barras e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte.

III - Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e dashboards da solução, possibilitando a alteração de eixos, título do gráfico, legenda, escala, rótulos de dados, tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código-fonte.

IV - Permitir aos usuários criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução.

V - Permitir a criação de gráficos com informações de diferentes entidades da solução, permitindo a sobreposição e cruzamento de informações e delimitação de linhas de tendência.

VI - Permitir que a partir de qualquer gráfico de gestão, contido em painéis e dashboards da solução, o usuário possa clicar e listar os registros relacionados com os dados contidos no gráfico (funcionalidade drill down).

VII - Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards de gestão, ajustando o layout e conteúdo do painel de acordo com suas necessidades.

VIII - Permitir aos usuários a configuração de painéis e dashboards agrupados por assunto e independentes entre si.

IX - Permitir ao usuário organizar seus painéis e dashboards com listas de registros de seu interesse, possibilitando a escolha de colunas, realização de filtros e ordenação da lista.

X - Permitir a geração de relatórios, impressão e exportação para arquivos no mínimo do tipo csv, html, pdf e xml.

XI - Prover informação em “real-time” de maneira gráfica por meio de dashboards.

XII - Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.

2.2.15. A solução deverá proporcionar as seguintes visões de controles/elementos:

I - Registro e Inventário de Dados;

II - Registro e Inventário dos servidores analisados;

III - Registros do DataMapping e Data Discovery (Dados estruturados e dados não estruturados), quando contratados;

IV - Painéis que apresentem de forma gráfica e com indicadores a Maturidade de TI.

V - Os elementos de controle da Lei.

2.2.16. A solução deverá prover um portal para que o titular possa exercer os seus direitos previstos na LGPD. Para cada entidade (CNPJ) do CONTRATANTE deverá ser previsto o portal do titular individualizado, permitindo a definição de qual DPO fará o atendimento das solicitações ocorridas neste portal. Os portais deverão usar o processo de autenticação com duplo fator (MFA), garantindo a autenticidade do titular em relação aos seus dados. O login deve ser o e-mail do titular, o qual ele usará para se cadastrar no portal durante seu primeiro acesso. As atividades executadas pelo titular dos dados no portal deverão ser registradas em protocolo, permitindo a rastreabilidade de todos os processos executados.

2.2.17. O sistema deve enviar um PIN de acesso temporário para o e-mail cadastrado no primeiro acesso ao portal do titular, desde que a CONTRATANTE possua dados referente a este titular. Essa informação deve ser passada ao titular após conclusão do cadastro.

2.2.18. Deve possibilitar o cruzamento de informações e controles em uma matriz de conformidade.

2.2.19. A solução deve permitir a edição de alguns itens da página do portal do titular, como:

I - Inserção de logo;

II - Informações sobre a empresa;

III - Hiperlink para política de privacidade e termos de uso

IV - Gestão de Consentimentos Obtidos;

V - Gestão de Terceiros;

VI - Criação e gestão de termos, políticas e normas;

VII - Gestão de Incidentes de Segurança/Não-conformidade;

VIII - Central de Informações do DPO;

IX - Mapa de Dados e dos Fluxos de Dados.

X - Diagnóstico de impacto e riscos, visando governança sobre:

a) Dados pessoais;

b) Dados sensíveis;

c) Framework de Governança e Orquestração de Processos;

d) Controles;

e) Riscos;

f) Políticas e Procedimentos (Diretrizes);

g) Afirmações das políticas;

h) Documentos normativos;

i) Citações;

j) Vulnerabilidade;

k) Conformidade;

l) Remediação;

m) Auditoria.

2.2.20. A solução deve permitir a integração com o portal "rj digital" através de login e senha pelo portal "gov.br"

2.3. **REQUISITOS DE COMUNICAÇÃO INTEGRADA**

2.3.1. Todas as atividades de uma organização devem estar ligadas com objetivos institucionais, com projetos, processos de trabalho e consequentemente devem estar vinculados com registros de gestão. A comunicação por meio de serviços de correio eletrônico e aplicativos de mensagens instantâneas externos, impede e dificulta o rastreamento de informações de projetos e processos de trabalho do CONTRATANTE. Com isso, é fundamental que a plataforma permita uma comunicação completa e integrada entre os atores envolvidos nas operações da LGPD. Para tanto, sem a necessidade de programação, a plataforma deverá:

I - Permitir a comunicação em tempo real entre clientes, usuários e atendentes dos serviços por meio de chat integrado à plataforma;

II - Permitir que a notações de trabalho sejam registradas nos registros da solução, dando a opção aos operadores atendentes de publicar e deixar visível ou não para usuários solicitantes.

III - Manter as partes interessadas e envolvidas nos processos e atendimentos dos serviços do CONTRATANTE informadas, é essencial para manter uma comunicação efetiva e um atendimento ágil. Para atender a essa necessidade, a plataforma deverá:

IV - Poder inserir notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados na solução;

V - Poder enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementa do na solução.

2.3.2. A velocidade exigida pelo negócio, tanto em operações da LGPD, quanto em operações de negócio do CONTRATANTE, também exige que Gestores, Técnicos e outros atores em processos e procedimentos, tenham a facilidade de uso e mobilidade para interagir com os processos da organização. Para tanto, é a solução deverá disponibilizar meios práticos e modernos de interação das pessoas com suas funcionalidades por meio de dispositivos móveis. Com isso, a solução deverá:

I - Ser responsiva para dispositivos móveis podendo ser operada por meio de aplicativos mobile que opere nos sistemas operacionais Android, IOS e Windows Phone;

II - Possuir funcionalidades, para usuários e operadores solucionadores, que permitam interações com aplicações, processos e fluxos de trabalho automatizados;

III - Poder tomar decisões e realizar ações que possam afetar os fluxos de um *workflow*;

IV - Poder visualizar e adicionar anexos;

V - Poder acessar menus configurados e personalizados na solução WEB;

VI - Possuir chat e mensagens instantâneas entre usuários da solução;

VII - Possuir notificações do tipo *push*.

2.4. **REQUISITOS DE SEGURANÇA**

2.4.1. A solução deve permitir a autenticação através do AD ou LDAP local da organização.

2.4.2. A solução deve permitir a criação de um login interno apenas se a conta existir no AD ou LDAP da organização.

2.4.3. A solução deve possuir mecanismo parametrizável de bloqueio da sessão e/ou logout automático por tempo de inatividade.

2.4.4. A solução deve prover mecanismo de segundo fator de autenticação.

2.4.5. Todas as funcionalidades da solução devem ser acessíveis através de um único login, sem necessidade de criação de logins adicionais.

2.4.6. A solução deve realizar o registro (logs) de todas as atividades ou tentativas de login/logout, registrando, no mínimo, a identificação do usuário, computador, data, hora e endereço IP utilizados.

2.4.7. A solução deve ter a funcionalidade de criação de perfis de DPO, TI (usuários administradores/aprovadores) e de usuário da plataforma, permitindo a criação desses papéis de acordo com as necessidades da contratante. Não poderá existir limitações de usuários preenchedores na plataforma.

2.4.8. Um perfil de acesso deverá ser composto de uma ou mais funcionalidades e/ou de um ou mais grupos.

2.4.9. A solução deve permitir a geração dos logs das atividades de administração da ferramenta e logs das atividades dos usuários, para fins de auditoria.

2.4.10. A solução deve permitir a consulta, pesquisa e geração de relatórios a partir dos logs de auditorias, conforme os itens de logs de auditoria especificados nesta seção.

2.4.11. A solução deve oferecer suporte para acesso de usuários externos, tais como fornecedores.

2.4.12. A criação de acesso para usuários externos deve ser controlada pelos administradores da solução, de forma que a identidade do usuário externo possa ser verificada antes da liberação do acesso.

2.4.13. A plataforma da solução deve possuir recursos para garantir a segurança das informações em trânsito e em repouso.

2.4.14. Quanto aos requisitos de segurança da aplicação, a solução deve atender, no mínimo, aos requisitos de segurança do framework OWASP (Open Web Application Security Project).

2.4.15. Quando fornecido em nuvem, o fabricante deverá comprovar por meio de certificações reconhecidas no mercado e relatórios de auditoria independente, a segurança de seu ambiente data center.

2.4.16. Os recursos de alta disponibilidade devem incluir, mas não se limitar a:

I - 99,8% de disponibilidade ou mais;

II - Centros de dados (Datacenters) espelhados localizados em território nacional;

III - Redundância total;

IV - Tolerância ao erro;

V - Balanceamento de cargas nos servidores;

VI - Monitoramento de desempenho;

VII - Processo de failover – RTO de 2 horas e RPO de 1 hora, no máximo;

VIII - Backup (Full) e recuperação de desastres;

IX - Plano de Continuidade de Negócios.

2.5. **REQUISITOS DE ATENDIMENTO AOS DIREITOS DOS TITULARES (DSAR)**

2.5.1. A solução deve ter capacidade para receber, processar e registrar uma solicitação de acesso dos titulares de dados, conforme exigido pela LGPD brasileira.

2.5.2. A solução deve permitir fluxos de atendimento distintos e configuráveis para cada tipo de solicitação.

2.5.3. A solução deve permitir alterar ou definir outro fluxo de atendimento durante a execução de uma solicitação.

2.5.4. A solução deve possuir um portal seguro onde o titular de dados pode entrar e visualizar o status do(s) seu(s) pedido(s) submetido(s), validando a identidade do titular.

2.5.5. Deverá fornecer 3 portais definidos pelo órgão para atendimento ao titular

2.5.6. A solução deve fornecer recursos de atribuição automática e reatribuição conforme necessário para cada ticket de solicitação de titulares.

2.5.7. A solução deve dispor de funcionalidade para selecionar e estender a solicitação do titular de dados.

2.5.8. A solução deve possuir fluxos de trabalho personalizáveis para processar todos as solicitações de titulares recebidos.

2.5.9. A solução deve possuir a funcionalidade de atribuir subtarefas dentro de uma solicitação de titulares.

2.5.10. A solução deve possuir formulários web personalizáveis onde os titulares de dados podem enviar seus pedidos.

2.5.11. A solução deve permitir que os titulares de dados possam enviar anexos nos formulários de solicitações, objetivando ajudar na verificação de sua identidade.

2.5.12. A solução deve possuir um painel de controle central para mostrar todas as solicitações recebidos em uma fila fácil de gerenciar.

2.5.13. A solução deve registrar através de um número de protocolo todas as atividades realizadas, permitindo rastrear o titular em cada solicitação.

2.5.14. A solução deve gerenciar e monitorar o tempo restante para cada solicitação ser atendida, além dos SLA definidos no workflow de aprovação da solicitação, notificando o DPO sempre que um SLA não for cumprido.

2.5.15. A solução deve fornecer protocolos de comunicação seguros com o titular de dados em relação ao seu pedido.

2.5.16. A solução deve fornecer modelos pré-definidos a serem usados para comunicação com um titular de dados referentes ao seu pedido, conforme os requisitos da LGPD.

2.5.17. A solução deve possuir recursos de geração de relatórios personalizados.

2.5.18. A solução deve registrar a entrega e o resultado de cada solicitação do titular de dados.

2.5.19. A solução deve registrar o fluxo, tempo e os fatores associados para cumprir o atendimento de cada solicitação.

2.5.20. A solução deverá permitir a integração do portal do titular com os processos de Data Discovery de dados estruturados e não estruturados, gerando as informações dos titulares de forma automática. Deverá permitir também a integração com os processos de negócio para busca de bases legais relacionadas ao titular.

2.5.21. A solução deverá permitir definir no portal do titular o DPO que será responsável pelo atendimento das solicitações realizadas neste portal, sendo que um DPO deverá poder ser cadastrado em mais de um portal. No registro da solicitação deverá ser identificado de qual portal veio a solicitação para o DPO.

2.6. REQUISITOS PARA GERENCIAMENTO DE NÍVEL DE SERVIÇO PARA AS SOLICITAÇÕES E ACOMPANHAMENTOS DOS DIREITOS DO TITULAR

2.6.1. A configuração de níveis de serviço adequados para todos os provedores de serviços internos e externos do CONTRATANTE é vital para garantir que a qualidade na prestação de serviços esteja alinhada com as necessidades de negócio. Para isso, a solução deverá:

I - Permitir a definição de parâmetros que são utilizados para definir o Service Level Agreement - SLA, tais como: por cliente, por serviço, dentro de um calendário a que se aplica o SLA, meta de nível de serviço relacionados ao SLA, escalações automatizadas relacionadas ao SLA.

II - Permitir a definição de critérios que possibilitem a associação de SLA a registros de atendimentos, incidentes, problemas, solicitações de mudanças e fluxos de trabalho do CONTRATANTE, automatizados na solução.

III - Permitir a definição de alertas com regras que viabilizem a emissão de avisos de registros incidentes, problemas, mudanças, solicitações de serviço, tarefas e atividades de fluxos de trabalho que estejam próximos de limites de SLA estabelecidos.

IV - Manter um histórico dos níveis mínimos de serviço para acompanhamento de desempenho dos serviços.

V - Permitir a definição do tempo de duração para os níveis mínimos de serviço ou percentual de disponibilidade de um item de configuração.

VI - Indicar quando o nível de serviço não foi cumprido ou está próximo do não cumprimento.

VII - Permitir definição de múltiplos SLA.

VIII - Permitir a criação de modelos de SLA para reutilização e facilidade de configuração de novos serviços.

IX - Possuir um repositório único com todos os registros de SLA, consolidando os Acordos de Nível de Serviço e Acordos de Nível Operacional.

X - Permitir o acesso seguro e controlado às informações do processo de gerenciamento de níveis de serviço e de SLA.

XI - Permitir gerenciar o ciclo de vida de SLA.

XII - Permitir anexar SLA á qualquer processo ou fluxo de trabalho do CONTRATANTE, automatizado na plataforma.

XIII - Implementar e seguir corretamente o fluxo de Gerenciamento de Níveis de Serviço conforme prescrito na biblioteca ITIL V3.

XIV - Deverá ser capaz de monitorar automaticamente os tempos de resposta, resolução e escalação relacionados com SLA.

XV - Deve permitir a configuração de contabilização de SLA apenas em horários definidos pelo CONTRATANTE, exemplo da necessidade de contabilização de SLA apenas em horas úteis.

XVI - Deve garantir o monitoramento dos prazos não apenas do SLA, firmado entre TI e usuários finais, mas também entre equipes (OLA) e prestadores de serviço externos (UC).

XVII - A medição de prazos deve ser insumo para a composição de indicadores gráficos de performance, exibidos em painéis do tipo dashboards.

XVIII - Permitir que eventos sejam disparados através da integração com ferramentas de monitoramento e gerenciamento de eventos e a contagem de seus prazos iniciados, para acompanhamento do atingimento dos limites definidos.

XIX - Permitir emitir relatórios das métricas de SLA sem a necessidade de outra solução.

XX - Deve permitir a automação da escalação e notificação, baseado nos tempos de resposta e resolução.

Garantir a integração nativa entre o Gerenciamento de Níveis de Serviço com o Gerenciamento de Incidentes, Problemas e Mudanças, garantindo que a execução de ações siga tempos pré-definidos.

XXI - Deve ser capaz de alertar ao time e à gestão, caso um evento exceda um número específico de atribuições e escalações.

2.7. REQUISITOS PARA GESTÃO DE CONSENTIMENTOS

2.7.1. A gestão do consentimento deve ser integrada aos demais componentes da solução, de forma a permitir o controle de quais processos/tratamentos usam consentimento, a finalidade do tratamento, quais dados e/ou dados sensíveis são tratados, o prazo de validade do tratamento.

2.7.2. Deverá permitir a gestão de consentimento para até um milhão de requisições por ano.

2.7.3. A solução deverá possuir API’s para integração dos processos de negócio da CONTRATANTE com o portal de consentimento da plataforma, devendo ser via portal Web e Smartphone.

2.7.4. Em complemento ao item anterior, a solução deve registrar os tratamentos de dados sensíveis e outras permissões realizadas através de consentimento.

2.7.5. Quando houver revogação de consentimento pelo titular, a solução deve notificar a necessidade de eliminação dos dados, exceto nas exceções previstas no art. 16 (o titular deve ter sido informado quanto às exceções de exclusão antes de fornecer o consentimento).

2.7.6. A Solução deve ser capaz de identificar os titulares que estão com o consentimento ativo e os titulares que solicitaram a revogação do consentimento.

2.7.7. A Solução deve controlar a validade do consentimento e solicitar novo consentimento ao usuário em caso de expiração.

2.7.8. A solução deve permitir a solicitação de novo consentimento caso uma nova finalidade de tratamento ou compartilhamento venham a ocorrer para os dados já coletados.

2.7.9. A Solução deve permitir que aplicações da contratante possam consultar o prazo de validade do consentimento.

2.7.10. A Solução deve permitir a consulta do histórico do consentimento concedido, por titular, data do consentimento, data da revogação do consentimento e sua finalidade. A consulta deve também ser disponibilizada ao titular pelo portal.

2.7.11. A Solução deve permitir realizar, no mínimo, as seguintes consultas: quais processos ou atividades possuem consentimento para uso de dados pessoais, quais são os sistemas que tratam esses dados, quais processos de negócio possuem consentimento para uso de dados pessoais, quantos titulares concederam o consentimento, e quantos titulares revogaram o consentimento.

2.7.12. A Solução deve fornecer um painel de controle central e recursos de relatórios que permitam ao DPO avaliar o status, histórico, estatístico e informações relacionadas de forma a verificar e comprovar a conformidade com o uso do consentimento para tratamento de dados pessoais e dados pessoais sensíveis realizados pela organização.

2.7.13. A solução deve permitir a integração do módulo de consentimento com as aplicações da contratante através de API, consolidando todos os consentimentos no portal da plataforma. A integração deve operar de forma bidirecional, permitindo que a aplicação seja informada quando o titular revogar o consentimento através do portal.

2.7.14. A solução deve possuir versão de aplicativo mobile para acesso e gestão dos consentimentos (opt-in e opt-out).

2.7.15. A solução deve gerar QR Code para redirecionamento para Plugin de site ou aplicativo de celular.

2.8. **REQUISITOS PARA GESTÃO DE TERCEIROS**

2.8.1. A solução deve permitir a avaliação de fornecedores e de terceiros.

2.8.2. A solução deve suportar a gestão de contratos e termos aditivos de fornecedores.

2.8.3. A solução deve permitir que os fornecedores acessem a aplicação usando um portal de autoatendimento.

2.8.4. A solução deve permitir que fornecedores respondam as avaliações via portal dentro da plataforma.

2.8.5. A solução deve possuir modelos pré-definidos de questionário de avaliação de fornecedores e permitir a customização desses modelos para criação de formulários de acordo com as necessidades da contratante.

2.8.6. A solução deve permitir a criação de questionários customizados a partir dos modelos existentes.

2.8.7. A solução deve prover a capacidade de auditar fornecedores externos de maneira personalizável.

2.8.8. O módulo de gestão de fornecedores deve permitir a geração de relatórios de gestão dos fornecedores.

2.8.9. A solução deve possuir um painel de controle para gestão dos fornecedores.

2.8.10. A solução deve permitir aos fornecedores que atuam como controladores conjuntos, registrar informações relativas às operações de tratamento sob sua responsabilidade.

2.8.11. O painel de controle de gestão de fornecedores deve permitir a criação de novos atributos para cada fornecedor de acordo com as necessidades da contratante.

2.8.12. A solução deve permitir aos fornecedores que atuam como operadores ou controladores conjuntos, consultar as informações relativas às operações de tratamento sob sua responsabilidade.

2.9. **REQUISITOS PARA GESTÃO DE RISCOS À PRIVACIDADE**

2.9.1. O sistema deve identificar os impactos para cada fluxo de dados de acordo com os critérios estabelecidos.

2.9.2. O sistema deve permitir o registro dos controles, das medidas, salvaguardas e mecanismos de mitigação de riscos identificados.

2.9.3. O sistema deve permitir o registro dos eventos e ameaças para o titular de dados, analisando a probabilidade de violação aos princípios da LGPD, o impacto que as violações podem causar ao titular em relação ao processamento dos dados pessoais.

2.9.4. O sistema deve emitir o relatório de impacto de proteção de dados (RIPD/DPIA).

2.9.5. O sistema deve permitir a criação de workflow e acompanhamento das atividades subsequentes relacionadas aos riscos, a fim de garantir execução dos controles corretivos.

2.9.6. A solução deve permitir o registro e a consulta de todas as atividades relacionadas às recomendações para mitigação dos impactos identificados no RIPD/DPIA (tratativas e recomendações com sucessos e sem sucessos), com a guarda do histórico.

2.9.7. O módulo de riscos deve possuir integração com o módulo de mapeamento de fluxo de dados para que as atualizações deste sejam refletidas na análise de impacto do fluxo de dados em questão.

2.9.8. O módulo de riscos deve possuir modelos de questionários/avaliações predefinidos que mapeiam especificamente os requisitos legais da LGPD, bem como deve permitir a importação de questionários criados pela CONTRATANTE.

2.9.9. Os questionários/avaliações devem suportar lógica condicional para o preenchimento.

2.9.10. A solução deve suportar pontuações de risco customizáveis.

2.9.11. A solução deve suportar a visualização dos riscos em um mapa de calor.

2.9.12. A solução deve suportar a avaliação quanto a eficácia dos controles aplicados aos riscos.

2.9.13. A solução deve suportar rastreamento de risco, sinalização e passos de mitigação de risco associados a cada incidente documentado.

2.9.14. A solução deve permitir filtros por criticidade e/ou nível de riscos para emissão do DPIA/RIPD.

2.10. **GESTÃO DE INCIDENTES DE VIOLAÇÃO**

2.10.1. A solução deve permitir o registro dos incidentes relativos à violação de dados pessoais, seja por acesso não autorizado ou por perda de informação como também outros tipos de incidentes.

2.10.2. A solução deve permitir o registro das identificações do incidente e seus atores, como a descrição, data de registro, identificação do relator, o período da ocorrência, os processos, documentos, aplicativos de negócios envolvidos, áreas envolvidas e empregados envolvidos.

2.10.3. A solução deve permitir o registro das informações referentes ao local do incidente; natureza da violação de dados (acesso não autorizado, perda acidental de dados pessoais etc.); quantidade de titulares envolvidos; quais os dados pessoais envolvidos, impacto para os titulares dos dados, para quem o incidente já foi reportado.

2.10.4. O sistema deve permitir a integração de API nativa com aplicações ITSM, tais como: ServiceNow, Citsmart, JIRA e BMC.

2.10.5. O sistema deve permitir o registro das consequências prováveis da violação de dados, todas as evidências do incidente, seja descritivo ou através de documentos anexados.

2.10.6. O sistema deve permitir o registro das ações tomadas para resolver o incidente e plano de tratamento do incidente.

2.10.7. O sistema deve armazenar o registro do fato que resultou a perda, indisponibilidade, divulgação ou alteração de dados pessoais.

2.10.8. O sistema deve registrar e permitir o acompanhamento e situação do incidente até o seu encerramento.

2.10.9. O sistema deve possuir um workflow em que o DPO faça a análise de todo o processo e realize a aprovação de encerramento do incidente.

2.10.10. O sistema deve permitir realizar as seguintes consultas: quantos incidentes foram abertos, concluídos em determinado período, quais os incidentes estão abertos, concluídos ou em andamento. Consulta detalhada do incidente com apresentação de todos os registros realizados (causa, impacto, ações tomadas, melhorias propostas, titulares envolvidos entre outros).

2.10.11. A solução deve gerar notificações automáticas por e-mail para as atividades dentro dos fluxos de trabalho.

2.10.12. A solução deve possuir fluxos de trabalho automatizados e customizáveis com subtarefas atribuíveis para cada incidente.

2.10.13. A solução deve suportar o rastreamento de risco, sinalização e passos de mitigação de risco associados a cada incidente documentado.

2.10.14. O módulo de incidentes da solução deve possuir formulário para comunicação do incidente à ANPD, conforme padrão https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, nativamente na solução, a fim de permitir rastreabilidade e acompanhamento do andamento do caso.

2.11. **GESTÃO DE AVISOS DE PRIVACIDADE E GESTÃO DE COOKIES**

2.11.1. O sistema deve possuir um módulo para criação, revisão, aprovação e publicação de políticas e avisos em websites e aplicativos, bem como controle do versionamento das políticas.

2.11.2. Deverá permitir a gestão de Cookies para até 50 (cinquenta) URLs fornecidas pelo órgão.

2.11.3. Deve atualizar as Políticas de Privacidade e Segurança de Dados Pessoais de todos os websites.

2.11.4. Deve fazer varreduras nos websites para verificar inconsistências nas Políticas de Privacidade e Segurança de Dados Pessoais.

2.11.5. Deve manter as versões antigas das Políticas de Privacidade e Segurança de Dados Pessoais.

2.11.6. Deve integrar as Políticas de Privacidade e Segurança de Dados Pessoais em aplicativos móveis através de SDK.

2.11.7. Deve permitir a criação das Políticas de Privacidade e Segurança de Dados Pessoais usando modelos pré-definidos, em conformidade com a LGPD e voltados para governo e empresas públicas.

2.11.8. Deve permitir a importação da Política de Privacidade e Segurança de Dados Pessoais atuais.

2.11.9. O sistema deve possuir um módulo para gestão de consentimento de uso de dados pessoais e de Cookies.

2.11.10. O sistema deve prever a gestão de consentimento para uso de cookies nos domínios da organização, através de varredura de páginas dos websites e coleta de consentimento para cada situação específica.

2.11.11. O sistema deve executar uma varredura para identificar todos os cookies e outras tecnologias de coleta de dados que estão sendo utilizadas nos websites.

2.11.12. Deve ser capaz de coletar recibos de ciência das Políticas para colaboradores e parceiros.

2.11.13. Deve ter capacidade de associar Políticas de Privacidade e Segurança da Informação aos controles existentes em seu programa de privacidade.

2.11.14. Deve permitir verificar o histórico de versões e fornecer notificações quando são feitas alterações nas políticas.

2.11.15. Deve ter capacidade de expor as Políticas associadas a um usuário num portal de autoatendimento.

2.11.16. Deve permitir a integração com sistemas de gestão de conteúdo já existentes.

2.11.17. Deve possuir recurso par bloquear automaticamente os cookies sem necessitar de "tag Managers".

2.11.18. Deve de capacidade de automatizar e realizar uma auditoria completa de todos os domínios do site de nossa organização.

2.11.19. Deve fornecer relatório ou descrição de uso para cada um dos cookies de terceiros e outras tecnologias de coleta de dados do site identificadas na varredura.

2.11.20. Deve fornecer relatório detalhando os resultados da auditoria de cookies, devendo incluir, mas não se limitar a:

I - Todos os cookies e instâncias de outras tecnologias de dados do site encontrados;

II - Identificar as tecnologias de captura de dados de cookies/site não declaradas nas políticas de cookies.

2.11.21. Deve ter capacidade de produzir uma política de cookies atualizada para cada domínio com base nos resultados da auditoria de cookies.

2.11.22. Deve ter a capacidade de criar um banner de cookie personalizado para cada site verificado.

2.11.23. Deve suportar diferentes idiomas para os banners de cookies.

2.11.24. Deve ter a capacidade de detectar automaticamente o idioma de preferência do visitante do site.

2.11.25. Deve de possuir recurso para suportar diferentes modelos de consentimento de cookies para que possamos escolher.

2.11.26. Deve ser capaz de registrar o consentimento de cookies dos visitantes do nosso site;

2.11.27. Deve permitir o agendamento periódicos de auditorias.

2.11.28. Deve notificar através de e-mail quando novos cookies forem identificados após uma varredura agendada e/ou iniciada manualmente.

2.11.29. Deve ter capacidade de reter relatórios de cookies para cada página verificada e rastrear as mudanças.

2.12. **MAPEAMENTO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS ATRAVÉS DE QUESTIONÁRIOS E INVENTÁRIO DE DADOS**

2.12.1. O módulo de mapeamento dos fluxos de dados pessoais (questionário de inventário) deve ser integrado aos demais módulos do sistema;

2.12.2. O módulo de mapeamento dos fluxos de dados (questionário de inventário) pessoais deve permitir o registro, atualização e consulta dos critérios utilizados para decisões automatizadas;

2.12.3. Deve possuir modelos de questionários pré-definidos que mapeiam especificamente os requisitos legais em regulamentos de privacidade brasileira;

2.12.4. Deve ter a capacidade de adicionar comentários por pergunta ao revisar o questionário preenchido;

2.12.5. Deve ter a capacidade permitir o envio de mensagens rápidas e interativas com os usuários preenchedores da plataforma, para dúvidas, registro de informações adicionais ou anexas.

2.12.6. Deve ter a capacidade de fazer upload de processos de negócios já analisados, sendo: Questionários de inventários, planos de ação, bases legais, etc.;

2.12.7. Deve possuir a funcionalidade de apoiar iniciativas de mapeamento de dados, incluindo mapeamento e análise de ativos e atividades de tratamento;

2.12.8. Deve ser capaz de armazenar informações sobre todos os itens acima, tais como classificação de atributos para cada ativo e atividade de processamento;

2.12.9. Deve possuir recurso para suportar diferentes elementos de dados que se aplicam a indivíduos específicos, tais como funcionários internos, clientes externos e fornecedores;

2.12.10. Deve ser capaz de atualizar o inventário de dados quando houver qualquer alteração nas quantidades, finalidades e demais características de ativos, processos ou atividades de tratamento de dados pessoais;

2.12.11. Deve possuir recursos para visualizações de mapeamento de dados, como mapas de calor e gráficos de dados pessoais pro processo;

2.12.12. Deve possuir a capacidade de gerar relatórios de acordo com o Artigo 37 da LGPD;

2.12.13. Deve possuir recurso que permita personalização dos relatórios de acordo com as necessidades da CONTRATANTE;

2.12.14. Deve possuir recuso para fazer reavaliação programada das atividades de mapeamento de dados;

2.12.15. Deve possuir recurso, como um painel de controle central, ou semelhante, com capacidade de classificação e filtragem;

2.12.16. Deve ter a capacidade de definir diferentes elementos de dados a serem associados a cada atividade de tratamento;

2.12.17. Deve permitir anexar documentos a um ativo ou atividade de tratamento individual;

2.12.18. Deve permitir o disparo de questionários para diversos respondentes via e-mail a partir da aplicação;

2.12.19. Deve permitir o envio de lembretes, via sistema e por e-mail, para os respondentes que receberam questionários para responder;

2.12.20. Deve permitir o envio de lembretes, via sistema e por e-mail, para os usuários cadastrados que tenham ações pendentes no sistema a serem executadas;

2.12.21. Deve registrar os riscos e controles aplicados a cada item do inventário (ativos, atividades de tratamento, fornecedores etc.);

2.12.22. Deve permitir a análise dos aspectos normativos de LGPD, definindo planos de ação, riscos, bases legais, teste de proporcionalidade do Legítimo Interesse, políticas, termos, normas e emissão do DPIA/LIA/ROPA;

2.12.23. A frequência e quantidade de lembretes devem ser preferencialmente, personalizáveis.

2.12.24. Deve permitir o mapeamento de dados em ambientes virtualizados.

3. SOLUÇÃO PARA DESCOBERTA DE DADOS ESTRUTURADOS E NÃO ESTRUTURADOS

3.1. A solução deverá ser licenciada com base na quantidade de equipamentos ou aplicações, devendo ser fornecida em blocos de 25 unidades de instâncias de banco de dados (dados estruturados) ou fontes de dados não-estruturados, até o total de 100 unidades.

3.2. Os produtos necessários ao atendimento dos requisitos dos componentes da solução deverão ser de um único fabricante ou estarem integrados nativamente sem a necessidade configurações que exijam codificação, exceto no caso de API.

3.3. A solução preferencialmente, na modalidade *on premise*, deve fornecer a possibilidade de instalação do core da aplicação em sistema operacional *open source* e que tenha a sua funcionalidade de rodar em contêiner. Caso a solução seja entregue na modalidade nuvem ou de forma hibrida, deve possuir uma nuvem própria ou utilizar de nuvens que atendam aos requisitos da ISO 27017.

3.4. Deve permitir integração nativa com fontes de dados estruturados:

I - Microsoft SQL Server 2008 ou superior;

II - MySQL;

III - PostgreSQL;
IV - DB2;
V - DB2 Mainframe;
VI - MariaDB;
VII - OracleDB;
VIII - Soluções de NoSQL;
IX - Aurora DB;
X - SAS;
XI - Vertica;
XII - SAP Hana.

3.5. Deve permitir integração nativa com fontes de dados semi-estruturados:
I - MongoDB.

3.6. Deve permitir integração nativa com fontes de dados não estruturados:
I - Microsoft Windows DFS;
II - Linux SMB;
III - EMC²;
IV - NetAPP;
V - AWS S3;
VI - Suite Office 365;
VII - Google Workspace.

3.7. Deve permitir integração nativa com:
I - Data Lakes & Data Warehouses;
II - Filas e Mensageria;
III - Bases Big Data & NoSQL;
IV - Aplicações;
V - Sistemas de Arquivos;
VI - Emails & Mensagens;
VII - Middleware;
VIII - Cloud SaaS;
IX - Cloud IaaS;

X - Mainframe;

XI - REST API.

3.8. Permitir desenvolvimento de Conectores Customizados.

3.9. Oferecer um inventario de todos os tipos de dados (tabelas, arquivos, filas etc.), atualizado de maneira continua e automática, com apoio de Machine Learning.

3.10. Deve contar com filtros (expressões) baseados no conteúdo e contexto (por exemplo, residências dos titulares vs geo-localização dos armazéns dos dados).

3.11. Permitir visualização das informações em mapas geográficos com as localizações dos sistemas e titulares.

3.12. Permitir visualização do estilo "mapa de calor" dos sistemas com mais dados pessoais e sensíveis.

3.13. Deve indicar a propriedade do objeto (donos, respectivamente técnicos e de negócio).

3.14. Permitir colaboração, como comentários nos objetos e possibilidade se seguir.

3.15. Permitir enfio de notificações de maneira proativa, sobre mudanças nos objetos, aos destinatários interessados (seguidores, donos, stewards etc.).

3.16. Deve indicar a correlação entre os dados armazenados em diferentes objetos, e conectá-los, junto com índice de confiança.

3.17. Permitir descobrimento de Dark Data (dados obscuros, até então desconhecidos) e Shadow IT.

3.18. Permitir realizar vista previa de conteúdo do objeto ou coluna, sem armazenar os dados.

3.19. Deve indicar pontuação de exposição ao risco, em diferentes níveis, como coluna, atributo, objeto, entidade, sistema fonte e organização.

3.20. Permitir classificação de objetos de acordo com os níveis de sensibilidade e criticidade do conteúdo.

3.21. Permitir classificação de dados PI (informação pessoal) e PII (informação de identificação pessoal).

3.22. Permitir a varredura de informações utilizando algoritmos de aprendizado de máquina em dados não-estruturados.

3.23. Permitir configuração das janelas e sistemas em quais especificas varreduras serão executadas.

3.24. Permitir iniciar, pausar, e parar uma varredura manualmente.

3.25. Permitir, através da interface do usuário, acompanhar o andamento das varreduras.

3.26. Permitir visualizar uma lista dos objetos com erro, para os quais a varredura não pôde ser executada.

3.27. Deve suportar o uso de expressões regulares para encontrar dados pessoais em dados estruturados e não-estruturados.

3.28. Deve suportar o uso da tecnologia OCR para classificar texto nos arquivos JPEG, JPG, BMP, GIF, PNG e PDF e imagens contidas dentro de arquivos Office.

3.29. Permitir manter uma lista de campos excluídos da análise, a serem ignorados pelas varreduras.

3.30. Deve possuir capacidade de aperfeiçoar o tempo de varredura de dados não-estruturados utilizando *machine learning*, de acordo com seus metadados.

3.31. Deve fazer a classificação e busca de dados dos titulares sem manter cópias ou índices dos dados.

3.32. Deve contar com, minimamente, as seguintes expressões regulares nativamente: (CPF, PIS, CNH, Título de Eleitor, IPv4, IPv6, IMEI, Email, Endereço MAC e Telefone).

3.33. Permitir a inclusão de novas expressões regulares e suportar a busca de termos próximos ao valor encontrado, para reduzir falsos positivos.

3.34. Deve suportar o treinamento de modelos de rede neural para classificar arquivos do negócio, como currículos, notas fiscais, *invoices* etc.

3.35. Deve ter a capacidade de adicionar *tags* (etiquetas) nas propriedades dos objetos para que outros sistemas possam identificar sua classificação.

3.36. Permitir customização dos *tags* (etiquetas) e aplicação automática de acordo com os critérios pré-estabelecidos ou padrões identificados através de *machine learning.*

3.37. Deve suportar a utilização de expressões regulares para classificação de metadados.

3.38. Deve ser possível realizar separadamente, a varredura de metadados, e de dados.

3.39. Deve construir um catálogo contendo todos os arquivos e tabelas escaneados durante as varreduras.

3.40. Permitir a exportação de seus dados em formato CSV.

3.41. Permitir a carga e a exportação de seus dados através de REST API.

3.42. Deve possuir capacidade nativa de intercâmbio com ferramentas de catalogação no mercado.

3.43. Deve ser capaz de indicar se um arquivo está duplicado em diversos sistemas.

3.44. Permitir agrupamento dos arquivos em grupos lógicos, que contém as mesmas características (fatura, CV, cartão de embarque etc.).

3.45. Deve ser capaz de indicar colunas similares, através de análise dos dados armazenados.

3.46. Permitir filtrar os resultados por sistemas, tipos de dados, classificação, existência de dados pessoais e duplicados.

3.47. Ao apresentar tabelas de bancos de dados relacionais, deve exibir suas colunas e o tipo de dados (declarado e inferido na base de conteúdo).

3.48. Ao apresentar tabelas de bancos de dados relacionais, deve indicar qual coluna é a chave primária, caso exista.

3.49. Ao apresentar tabelas de bancos de dados relacionais, deve indicar a qualidade de dados por coluna: tipo inferido, % distintos, % nulos, valores min/max etc.

3.50. Ao apresentar arquivos, o catálogo deve indicar se possui permissões excessivas, como visualização ou edição, grupos *Everyone*, *Domain Users*, e *Authenticated Users*.

3.51. Deve contar com dashboard que permita visualizar de forma prática a quantidade de objetos com permissões excessivas.

3.52. Deve contar com dashboard que permita visualizar de forma prática quais sistemas possuem mais arquivos com permissões excessivas.

3.53. Deve contar com dashboard que permita visualizar de forma prática quais sistemas possuem arquivos compartilhados com usuários externos à organização.

3.54. Deve contar com dashboard que permita visualizar de forma prática quantas políticas de conformidade estão sendo atendidas ou infringidas.

3.55. Permitir descobrimento quais dados são afetados por regulamentações com política pré-configuradas prontas para uso.

3.56. Permitir criação de novas políticas e customização das existentes.

3.57. Permitir configuração de gatilhos e critérios quantitativos (de violações).

3.58. Permitir identificação automática das quais políticas se aplicam as quais dadas confidenciais e sensíveis.

3.59. Permitir revalidação das políticas a cada atualização (metadados ativos).

3.60. Permitir aplicação de *tags* (etiquetas) relacionadas com políticas *out-of-the-box*.

3.61. Permitir aplicação de *tags* (etiquetas) relacionadas com políticas customizadas.

3.62. Permitir auditoria e ações automáticas de acordo com as regras das políticas, e notificações.

3.63. Permitir aplicação de novas políticas em escala à medida que as regulamentações mudam ou novas regulamentações são introduzidas.

3.64. Deve possuir mecanismo para acionar APIs de outros sistemas a partir da violação de uma política.

3.65. Deve fornecer relatórios de avaliação das varreduras, a estrutura, e logs.

3.66. Permitir avaliação e exportação dos resultados das varreduras em relatórios detalhados.

3.67. Permitir integração aberta com aplicações e sistemas do CONTRATANTE.

3.68. Permitir integração com outros catálogos de dados e qualquer sistema fonte.

3.69. Deve oferecer bibliotecas SDK para desenvolvimento customizado de novos módulos e conectores.

3.70. Permitir disponibilização do conteúdo do catálogo aos cientistas de dados em bibliotecas Python.

3.71. Deve contar com tecnologia de repositório de metadados com opção de replicação e alta disponibilidade nativa.

3.72. Deve possuir opção de comunicação segura entre todos seus componentes, com criptografia SSL e certificados.

3.73. Permitir arquitetura distribuída compreendendo ambientes híbridos, *multi-cloud*, e *multi-datacenter*.

3.74. Permitir escalonamento horizontal sob demanda para atender tarefas computacionais intensas, como *scans.*

3.75. Permitir instalação remota dos scanners para realizar varreduras perto das fontes e minimizar a transferência de dados e custos de *data regress*, quando aplicável.

3.76. Permitir (arquitetura aberta) desenvolvimento customizado, para ampliação das funcionalidades nativas, como criação de novo módula e conectores adicionais.

3.77. Permitir integração com provedores de identidade IDM através de protocolo SAML ou LDAP para autenticação de usuários.

3.78. Deve utilizar RBAC (com possibilidade de customização) para definir diferentes perfis de acesso às funcionalidades do sistema.

3.79. Permitir a criação de escopos para limitar quais sistemas e dados são visíveis aos quais usuários.

3.80. Deve possuir auditoria dos acessos realizados, seja através da interface de usuário ou diretamente através de API.

3.81. Deve possuir a opção de exportar os logs do sistema e de auditoria através da interface de usuário.

3.82. Deve ser disponibilizada através de protocolo web, para acesso através de navegadores.

3.83. Deve ser compatível minimamente com os seguintes navegadores: Google Chrome, Apple Safari e Mozilla Firefox.

3.84. Deve oferecer um dashboard para acompanhamento dos principais indicadores da solução.

3.85. Deve oferecer um dashboard que fornece recursos gráficos como mapas e gráficos para melhor visualização das informações.

3.86. Deve oferecer um dashboard que fornece atalhos para os principais recursos da solução e atividades.

3.87. Permitir salvar as consultas e filtros, para que sejam refeitas de maneira prática posteriormente.

3.88. Permitir envio de notificações por e-mail sobre novas atividades designadas.

3.89. Permitir envio de notificações por e-mail sobre o andamento das varreduras.

3.90. Permitir envio de notificações por e-mail sobre políticas em não-conformidade.

3.91. **REQUISITOS DO MÓDULO DE GOVERNANÇA DE DADOS**

3.91.1. Permitir análise de linhagem de dados, ao nível de objeto, para entender e rastrear a origem e como a informação foi transformado.

3.91.2. Permitir análise de linhagem de dados, ao nível de coluna, para entender e rastrear a origem e como a informação foi transformado.

3.91.3. Permitir realizar a análise de impacto, ao nível de objeto, para evolução proativa de impactos diretos e indiretos das mudanças planejadas.

3.91.4. Permitir realizar a análise de impacto, ao nível de coluna, para evolução proativa de impactos diretos e indiretos das mudanças planejadas.

3.91.5. Permitir integração com ferramentas terceiras especializadas em linhagem dedada, como por exemplo, Manta.

3.91.6. Permitir geração de linhagem derivada dos dados e correlações e não somente dos metadados de integração e transformação.

3.91.7. Permitir acompanhamento da mudança dos indicadores de qualidade de dados ao longo do processo de transformação.

3.91.8. Permitir diferentes níveis de visão, desde linhagem detalhada até visão agregada e simplificada para melhor entendimento.

3.91.9. Permitir exportação da linhagem de dados e relatórios da análise de impacto.

3.91.10. Permitir criação manual de linhagem de dados, além das integrações com ferramentas terceiras.

3.91.11. Deve oferecer um gerenciador de tarefas para que os Stewards possam priorizar e organizar o trabalho.

3.91.12. Devem permitir colaboração entre Stewards, proprietários de negócios e proprietários técnicos.

3.91.13. Permitir agrupamento de tarefas de administração semelhantes para processamento em lote.

3.91.14. Deve usar *Machine Learning* para recomendar invés de selecionar manualmente os glossários de negócios.

3.91.15. Permitir associação automática dos termos lógicos do glossário com ativos físicos em escala.

3.91.16. Permitir pesquisa de glossário comercial para que os usuários encontrem termos e atributos.

3.91.17. Permitir criação de hierarquias de domínios, atributos, termos para estrutura e compreensão.

3.91.18. Permitir importação dos termos do glossário comercial de fontes de terceiros.

3.91.19. Permitir enriquecer os catálogos de terceiros com termos do glossário.

3.91.20. Permitir enriquecer os catálogos de terceiros associando termos lógicos do glossário a dados físicos.

3.91.21. Permitir identificar automaticamente as informações pessoais e confidenciais em todos os ativos de dados.

3.91.22. Permitir captura da finalidade de uso para justificação de armazenamento destes dados.

3.91.23. Permitir mapeamento dos termos lógicos do glossário de negócios para ativos físicos.

3.91.24. Devem permitir definição de regras personalizadas de qualidade de dados.

3.91.25. Permitir gestão de regras de qualidade de dados em linguagem natural.

3.91.26. Permitir tomar ações para os dados que não cumprem esperados níveis de qualidade.

3.91.27. Permitir notificar aos proprietários dos dados sobre eventos de avaliação e resultados.

3.91.28. Permitir avaliação com o Machine Learning para obter orientação sobre valores discrepantes.

3.91.29. Permitir avaliação de regras de qualidade dos dados por colunas.

3.91.30. Permitir avaliação de regras de qualidade dos dados por atributos (por exemplo CPF, e-mail, RG etc.).

3.91.31. Permitir avaliação de regras de qualidade dos dados por objeto (tabela, coluna etc.).

3.91.32. Permitir gerenciamento proativo de qualidade de dados.

3.91.33. Permitir definição de regras reutilizável no nível organizacional, para gerenciar qualidade em fontes de dados, projetos e iniciativas.

3.91.34. Permitir acompanhamento das tendências da qualidade na linha de tempo.

3.91.35. Permitir gerenciamento de qualidade dos dados a partir de um único ponto de controle.

3.91.36. Deve integrar para o catálogo as pontuações de níveis de qualidade de dados.

3.91.37. Permitir integração com as tecnologias de fluxo de trabalho.

3.91.38. Permitir definição de políticas para gerenciamento do ciclo de vida dos dados.

3.91.39. Permitir definição de políticas para retenção legal (ex. dados dos ex-funcionários, ações na justiça).

3.91.40. Permitir criação de políticas em critério de tempo (filtro de data).

3.91.41. Permitir criação de políticas em critério de metadados (ex. data de criação do documento, modificação etc.).

3.91.42. Permitir criação de políticas em critério de classificação (atributos, sensibilidade etc.).

3.91.43. Permitir análise automática de todos os dados para identificar quaisquer dados que violem as políticas.

3.91.44. Permitir ações sobre os dados que precisam ser arquivados ou excluídos (remediação).

3.91.45. Permitir exportação e importação de políticas.

3.92. **REQUISITOS DO MÓDULO DE PRIVACIDADE DE DADOS**

3.92.1. Permitir a emissão de relatório de acesso aos dados do titular (dossiê), personalizado, com todas as informações relacionadas ao titular.

3.92.2. Permitir a busca de dados pessoais iniciadas através do nome ou código único de identificação, como o CPF.

3.92.3. Permitir rastreamento dos dados pessoais retornados pelo inventário na busca de um titular até a tabela onde foram encontrados.

3.92.4. Permitir rastreamento dos dados pessoais retornados pelo inventário na busca de um titular até o arquivo onde foram encontrados.

3.92.5. Permitir a requisição e obtenção do dossiê através de API.

3.92.6. Permitir inclusão no dossiê também dos registros de consentimento coletados do titular.

3.92.7. Permitir deleção de dados sobre solicitação do titular ou gestão de fluxo de trabalho com controle de tarefas manuais.

3.92.8. Permitir emissão do dossiê em formato PDF ou CSV.

3.92.9. Deve fazer a busca de dados do titular automaticamente (sem intervenção) e sob demanda, buscando sempre os dados mais atuais nas fontes de dados.

3.92.10. Permitir solicitações em lotes, por mais que um titular numa solicitação.

3.92.11. Permitir diferentes perfis de dossiê, de acordo com o relacionamento com o titular, exemplos: funcionário, ex-funcionário, CONTRATANTE, fornecedor etc.

3.92.12. Deve contar com um mecanismo que garanta que os dados foram de fato excluídos e que permaneçam excluídos, mesmo em caso de restauração de backup, por exemplo.

3.92.13. Deve prover um portal de autoatendimento para que o próprio titular possa realizar suas solicitações.

3.92.14. Permitir, no mínimo, solicitações de acesso, retificação e remoção dos dados, bem como alteração das preferências de consentimento.

3.92.15. Deve possuir integração com protocolo OAUTH para autenticação dos solicitantes.

3.92.16. Permitir controles de segurança como confirmação positiva de e-mail e telefone para validação dos dados.

3.92.17. Permitir customização do questionário de solicitação.

3.92.18. Permitir envio de imagens e documentos para comprovação da identidade do solicitante.

3.92.19. Permitir a configuração de fluxos de trabalho, possibilitando inclusive a entrega completamente automatizada do relatório final para o titular.

3.92.20. Deve fornecer dashboard para que o gestor de privacidade possa ter uma visão agrupada das requisições, minimamente: data, tipo da solicitação, e prazo/em atraso.

3.92.21. Deve fornecer ao titular uma interface com os dados originais e permiti-lo alterar estes dados.

3.92.22. Permitir ao gestor a revisão das informações antes de serem enviadas ao solicitante.

3.92.23. Deve possuir auditoria das solicitações, dos revisores e dos aprovadores.

3.92.24. Deve ser capaz de ler diversas fontes de consentimento para identificar quais consentimentos foram dados por cada titular.

3.92.25. Permitir documentação dos termos de privacidade disponíveis, com sua localização (URL), versão e tempo de validade, relacionando-os às bases legais.

3.92.26. Permitir emissão de um relatório das bases legais, e quais dados estão relacionados a elas.

3.92.27. Permitir emissão de um relatório de propósitos de utilização, e quais dados estão relacionados a eles.

3.92.28. Permitir registro, gestão, validação de consentimento do titular.

3.92.29. Permitir integração de base externa com registros de consentimento.

3.92.30. Permitir documentação dos termos legais de consentimento.

3.92.31. Permitir documentação do propósito de armazenamento dos dados.

3.92.32. Permitir documentação da base legal para armazenamento de dados.

3.92.33. Dever permitir múltiplos canais de consentimento (CONTRATANTE, fornecedores, funcionário etc.).

3.92.34. Devem permitir customização de acordos, baseados em regulamentações ou políticas internas.

3.92.35. Deve oferecer ao titular centro de gestão de preferências.

3.92.36. Devem correlacionar automaticamente os consentimentos e preferências.

3.92.37. Deve identificar todos os cookies e outras tecnologias de coleta de dados estão sendo utilizadas nos sites.

3.92.38. Deve incluir a auditoria de páginas web onde a autenticação do usuário é necessária.

3.92.39. Deve fornecer uma descrição de uso para cada um dos cookies de terceiros e outras tecnologias de coleta de dados do site identificadas na varredura.

3.92.40. Deve possuir a capacidade de gerar relatórios: todos os cookies e instâncias de outras tecnologias de dados do site encontrados.

3.92.41. Deve possuir a capacidade de gerar relatórios: identificar as tecnologias de captura de dados de cookies/site não declaradas nas políticas de cookies.

3.92.42. Deve possuir a capacidade de produzir uma política de cookies atualizada para cada domínio com base nos resultados da auditoria de cookies.

3.92.43. Deve possuir a capacidade de criar um banner de cookies personalizado para cada site verificado.

3.92.44. Deve possuir a capacidade de que o banner de cookies para cada domínio seja "estilizado" de forma diferente de acordo com as orientações da marca desse domínio.

3.92.45. Deve registrar o consentimento de cookies dos visitantes dos sites.

3.92.46. Deve possuir a capacidade de adicionar uma descrição de cookies novos/desconhecidos antes da política de cookies ser publicada.

3.92.47. Permitir que realização das auditorias automatizadas não degrade ou prejudica o desempenho em tempo real dos sites auditados.

3.92.48. Permitir auditorias automatizadas realizadas pelo menos a cada trimestre.

3.92.49. Deve possuir a capacidade de reter relatórios de cookies para cada página verificada e rastrear as mudanças.

3.92.50. Deve possuir a capacidade de bloquear automaticamente os cookies das categorias as quais o visitante não deu consentimento.

3.92.51. Permitir mapeamento de processos de negócios, atores, bases de dados e aplicações envolvidas.

3.92.52. Permitir gestão e visibilidade de atividades de processamento de dados.

3.92.53. Permitir monitoramento das atividades de processamento de dados.

3.92.54. Permitir sinalizar riscos relacionados com envolvimento de dados confidenciais e sensíveis.

3.92.55. Permitir criação de modelos padrão de processamento de dados a partir das descobertas realizadas.

3.92.56. Permitir carregamento manual dos modelos de processamento de dados.

3.92.57. Permitir descobrimentos de compartilhamento de dados com terceiros.

3.92.58. Permitir documentação de compartilhamento de dados com terceiros.

3.92.59. Permitir geração de relatórios de processamento de dados.

3.92.60. Permitir geração de relatórios de compartilhamento de dados com terceiros.

3.92.61. Permitir avaliação de risco dos processos de negócios.

3.92.62. Permitir gestão da conformidade com regulamentações.

3.92.63. Permitir revisão e aplicação das recomendações sobre processos de negócio para agilizar a documentação.

3.92.64. Permitir exportação da documentação dos processos em formato PDF, ou semelhante.
3.92.65. Permitir mapear e documentar fluxos de risco de privacidade.
3.92.66. Permitir mapear e documentar a estrutura organizacional de privacidade.
3.92.67. Permitir avaliação de risco relacionado aos terceiros.
3.92.68. Permitir colaboração na avaliação de risco.
3.92.69. Permitir medição níveis de acessos e exposição pública.
3.92.70. Permitir documentação das transferências de dados.
3.92.71. Deve alterar em função de acionamento dos gatilhos de nível de risco.
3.92.72. Permitir gestão de fluxos de trabalho de correção de dados (remediação).
3.92.73. Deve oferecer as trilhas de auditoria e relatórios.

3.93. **REQUISITOS DO MÓDULO DE SEGURANÇA DE DADOS**
3.93.1. Permitir identificação dos usuários e contas com privilégios excessivos;
3.93.2. Permitir identificação dos dados superexpostos por sensibilidade;
3.93.3. Deve fornecer a visibilidade de acessos no nível interno e externo, por sensibilidade;
3.93.4. Deve sinalizar e permitir investigação dos problemas de alto risco;
3.93.5. Deve integrar para o catálogo os objetos com acessos ou permissões excessivas;
3.93.6. Permitir integração com ferramentas como MIP e DLP para reforçar o cumprimento;
3.93.7. Permitir correção dos conjuntos de dados com violações e problemas de risco, com orquestração de fluxo de trabalho;
3.93.8. Deve priorizar as descobertas por sensibilidade e nível de risco de exposição;
3.93.9. Permitir atribuir atividade de correção relacionada com conjuntos de dados;
3.93.10. Permitir delegar as atividades de correção por função, escopo e usuário;
3.93.11. Permitir automação de ações de remediação como deleção, quarentena;
3.93.12. Permitir coleção de informações para trilha de auditoria das ações tomadas;
3.93.13. Permitir colaboração entre as equipes e comentários;
3.93.14. Permitir integração com ferramentas terceiras (ex: anonimização, criptografia, aposentadoria etc.)
3.93.15. Permitir integração com ferramentas como MIP e DLP para reforçar o cumprimento;
3.93.16. Permitir carregamento de amostra de dados vazados para análise do conteúdo e identificação dos titulares envolvidos;
3.93.17. Permitir carregamento de amostra de dados vazados para identificação (pela sua semelhança) qual dos sistemas monitorados foi possivelmente comprometido;
3.93.18. Permitir evolução e pontuação de risco de exposição de acordo com os dados vazados;
3.93.19. Permitir identificação de dados regulamentados superexpostos;
3.93.20. Permitir identificação e monitoramento contínuo de dados confidenciais superexpostos;
3.93.21. Permitir identificação dos usuários com privilégios excessivos;

3.93.22. Permitir identifique de dados confidenciais e sensíveis duplicados (superfície de ataque);

3.93.23. Permitir atribuição de pontuações de risco com base na fonte de dados;

3.93.24. Permitir atribuição de pontuações de risco por tipo de dados (classificação de atributos);

3.93.25. Deve permitir atribuição de pontuações de risco por país de residência do titular.

4. SOLUÇÃO PARA AVALIAÇÃO, CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA

I - A solução deverá ser licenciada com base na quantidade de usuários, devendo ser fornecida para atender a até 1000 usuários.

II - Os produtos necessários ao atendimento dos requisitos dos componentes da solução deverão ser de um único fabricante ou estarem integrados nativamente sem a necessidade configurações que exijam codificação, exceto no caso de API.

4.1. REQUISITOS DE SIMULAÇÃO DE PHISHING

4.1.1. O componente deverá ser provido em nuvem do fabricante e não deve ser exigir nenhum servidor adicional, IP dedicado para disparos de e-mail, tão pouco registro de domínios para a sua plena execução.

4.1.2. Plataforma de administração deve suportar HTTP e HTTPS.

4.1.3. Plataforma de usuário para os treinamentos deve suportar no mínimo inglês e português do Brasil sendo o conteúdo dos treinamentos em português do Brasil.

4.1.4. Deve suportar integração com Azure Active Directory e LDAP Active Directory.

4.1.5. Deve prover os seguintes módulos/funcionalidades através da mesma console:

I - Customização e Simulação de Phishing via e-mail;

II - Customização e Simulação de Phishing via USB;

III - Treinamentos;

IV - Exames e Testes;

V - Relatórios e Indicadores;

VI - Materiais adicionais como cartilhas, papel de paredes, vídeos, etc.

4.1.6. Os treinamentos oferecidos pelo componente devem obrigatoriamente ser:

I - Módulos Interativos;

II - Possuir duração mínima de 5 minutos, cada;

III - Ser providos em português.

4.1.7. Não deve haver restrição de volume de e-mail phishing enviados durante o contrato vigente.

4.1.8. Deve ser possível criar campanhas de Phishing com as mínimas características:

I - Campanhas no formato texto e HTML;

II - Campanhas com arquivos anexos (PDF, WORD, EXCEL, HTML no mínimo);

III - Campanhas com arquivos anexos comprimidos (formato ZIP) e com senha.

4.1.9. O componente deverá prover templates de e-mail phishing prontos para serem utilizados.

4.1.10. O componente deverá possibilitar a criação de templates e-mail phishing conforme a necessidade.

4.1.11. Não deve haver restrição de quantidade de templates e-mail phishing que podem ser criados.

4.1.12. O componente deverá prover uma lista de domínios próprios que podem ser utilizados nas simulações, sem qualquer ônus adicional para a sua utilização.

4.1.13. Os domínios disponíveis devem abranger, no mínimo, as seguintes categorias:

I - domínios corporativos;

II - domínios técnicos;

III - domínios redes sociais;

IV - domínios comerciais;

V - domínios financeiros;

VI - domínios e-commerce.

4.1.14. Deve ser possível simular um phishing realizando um ataque do tipo domain spoofing, ou seja, deve ser possível utilizar o mesmo domínio da empresa para disparos de e-mails simulação de phishing.

4.1.15. Deve ser possível criar subdomínio no link da simulação de Phishing, como por exemplo, https://subdominio.teste.com.br.

4.1.16. Deve ser possível ajustar o endereço URL utilizado no e-mail Phishing, como por exemplo, www.urlphishing.com.br/login.php.

4.1.17. Deve ser possível ajustar os principais campos no e-mail como:

I - Assunto;

II - E-mail Origem (campo FROM);

III - E-mail Retorno (campo Reply-To);

IV - Alias.

4.1.18. Deve ser possível criar um e-mail através de wizard ou HTML.

4.1.19. Deve ser possível trabalhar com, no mínimo, as seguintes variáveis de sistema para uma melhor automação:

I - Nome;

II - Sobrenome;

III - Endereço de E-mail;

IV - Data;

V - Hora.

4.1.20. O componente deverá prover um banco de imagens para serem utilizados nas campanhas de Phishing.

4.1.21. O componente deverá suportar o envio randômico de uma ou mais campanhas de phishing levando em consideração a quantidade de usuários a ser enviado.

4.1.22. A funcionalidade randômica deve ser configurada em data início e fim, dias da semana e horários início e fim.

4.1.23. Deverá ser possível agendar o envio das campanhas de phishing conforme uma data pré-definida.

4.1.24. Deverá ser possível definir o tempo que a URL utilizada na campanha de Phishing fique disponível e acessível.

4.1.25. Deverá possibilitar a coleta do comportamento dos usuários internos de forma anônima para atender a quesitos legais como a Lei Geral de Proteção de Dados ou outra.

4.1.26. Deverá ser possível a customização da página utilizada na simulação da fraude.

4.1.27. Deverá ser possível coletar informações de geolocalização.

4.1.28. As simulações de phishing devem ser compatíveis com os principais sistemas operacionais de mercado como Windows, Mac, Linux e dispositivos, como Android, IOS smartphone, tablet e outros.

4.1.29. Deverá registrar o endereço IP de onde o usuário final abriu o phishing.

4.1.30. Deverá registrar de qual dispositivo ou computador ou sistema operacional que o usuário final abriu o phishing.

4.1.31. Deverá registrar de qual navegador web o usuário abriu o Phishing.

4.1.32. Deverá ser possível exportar os resultados via CSV.

4.1.33. Deverá ser possível acompanhar o andamento da campanha via portal.

4.1.34. Deverá ser possível a criação de arquivos para a simulação de phishing por USB, onde será possível analisar comportamento de usuários internos obtendo acesso a pendrives desconhecidos.

4.2. **REQUISITOS DA PLATAFORMA DE TREINAMENTO**

4.2.1. O componente deverá disponibilizar módulos de treinamentos em Português (Brasil).

4.2.2. Deverá ser provido treinamentos em vídeos e módulos interativos.

4.2.3. Deverá possuir diferentes módulos de treinamentos, tais como:

I - Identificação de links fraudulentos;

II - Identificação de e-mail phishing;

III - Senha Seguras;

IV - GDPR e LGPD;

V - Segurança Física;

VI - Protegendo dados Confidenciais;

VII - Segurança em Redes Sociais.

4.2.4. Deverá possibilitar a customização dos treinamentos existentes para logo da empresa e imagens diferentes do provido pela solução.

4.2.5. Deverá possibilitar a customização do conteúdo dos treinamentos conforme a necessidade.

4.2.6. Deverá ser possível configurar data início e fim para a realização dos treinamentos.

4.2.7. Deverá ser possível aplicar mais de um módulo de treinamento por grupo de usuários.

4.2.8. Deverá ser possível enviar notificações por e-mail, pré-agendadas, de alerta ao usuário de que existem treinamentos pendentes e/ou novos para serem realizados.

4.2.9. Deverá ser possível a customização das notificações.

4.2.10. Deverá ser possível vincular os módulos de treinamentos para um usuário ou um grupo de usuários pré-configurado no Active Directory (AD).

4.2.11. Deverá ser possível configurar um certificado virtual quando usuário final obtiver sucesso no término de um curso.

4.2.12. Deverá suportar a exportação dos módulos de treinamento via SCORM, no mínimo, nas versões 1.2 e 2004.

I - Funcionalidades de testes e exames:

a) O componente deverá possuir um banco de perguntas e resposta com no mínimo 400 perguntas.

b) O componente deverá disponibilizar perguntas e respostas em inglês e português.

c) Deverá possibilitar a criação de questões novas, conforme a demanda.

4.2.13. Com relação às perguntas novas:

4.2.14. Deverá ser configurável em verdadeiro/falso ou múltiplas escolhas;

I - Deverá ser multilíngue;

II - Deverá possibilitar importar imagens para uma melhor ilustração.

4.2.15. Deverá ser possível criar categorias de perguntas e respostas.

4.2.16. Para cada categoria, deverá possuir a opção de alternar as perguntas para nunca seguir uma sequência repetitiva de mesma questão.

4.2.17. Deverá ser possível aplicar diferentes categorias de perguntas para diferentes grupos de usuários.

4.2.18. Relatórios e Indicadores:

I - Deverá suportar exportar relatórios nos formatos Excel, CSV e PDF.

II - Deverá prover Dashboard centralizado.

III - Deverá possuir filtros para uma dinâmica visualização.

IV - Deverá possuir, no mínimo, os seguintes relatórios:

a) Detalhes das campanhas de phishing;

b) Taxa de falhas por campanha de phishing e por usuário;

c) Comparação de efetividade entre campanhas de phishing;

d) Detalhes individuais de cada campanhas como:

e) Nome do usuário;

f) Tipo de endpoint;

g) Localização Geográfica;

h) Comportamento individual.

i) Taxa de sucesso e falhas nos testes;

j) Tempo médio de execução do treinamento;

k) Usuários que não realização os treinamentos.

4.2.19. Deverá ser possível realizar agendamentos para entrega de relatórios para uma lista de distribuição de e-mail

4.2.20. Os relatórios deverão ser acessados através da mesma console de administração do componente e não serão aceitos qualquer modulo ou serviço adicional que dependa de qualquer recurso adicional.

5. SOLUÇÃO PARA GESTÃO DE ATENDIMENTO A TITULARES, DENÚNCIAS E GOVERNANÇA DE CERTIFICADOS EM CONFORMIDADE COM A LGPD

I - A solução deverá ser licenciada para acesso de até 25 usuários.

II - Os produtos necessários ao atendimento dos requisitos dos componentes da solução deverão ser de um único fabricante ou estarem integrados nativamente sem a necessidade configurações que exijam codificação, exceto no caso de API.

III - Caso venha a ser fornecida em nuvem, a CONTRATADA deverá comprovar que toda a comunicação bem como o ambiente fornecido pelo fabricante é seguro e atende às boas práticas de mercado.

IV - Toda a comunicação com a solução deverá ocorrer utilizando-se de recursos criptográficos, assim como os dados deverão ser armazenados em banco de dados criptografados.

5.1. REQUISITOS GERAIS

5.1.1. A automação de processos e fluxos de trabalho da solução deve ser interativa, prática e de fácil implementação. O desenvolvimento de soluções ágeis e dentro da velocidade que o negócio da CONTRATANTE exige, deve ser suportado pela solução, para tanto, a solução deve suportar a criação de soluções, automações de fluxos de trabalho, processos de TI e de negócio e suportar a implementação de rotinas e processamento de funcionalidades com uma programação mínima e básica (Low-Code), usando componentes integrados e nativos da própria plataforma.

5.1.2. A solução deverá ser ofertada na modalidade Software como Serviço - SaaS, em nuvem com Data Centers localizados exclusivamente em território nacional, sem qualquer replicação de dados no exterior.

5.1.3. Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados em decorrência da prestação de serviços, bem como suas cópias de segurança, residam em território brasileiro, para tanto, a empresa contratada deve garantir a territorialidade única na prestação do serviço, em vez de um ambiente tecnológico multinacional, não sendo admitida nenhum tipo de replicação para fora do país, tão pouco o fornecimento de informações.

5.1.4. Deverão ser garantidos a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade dos conhecimentos, informações e dados hospedados em ambiente tecnológico sob custódia do prestador de serviços.

5.1.5. Garantia de que o acesso aos dados, metadados, informações e conhecimentos utilizados e/ou armazenados na solução, ferramentas, softwares, infraestrutura ou em qualquer outro recurso que a empresa contratada utilize para a prestação de serviços somente serão acessados pela CONTRATANTE e serão protegidos de acessos não autorizados.

5.1.6. Garantia que, em qualquer hipótese, a CONTRATANTE tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços.

5.1.7. Vedado o uso não corporativo dos conhecimentos, informações e dados pelo prestador de serviço, bem como a replicação não autorizada.

5.1.8. A empresa contratada deve executar os serviços em conformidade com a legislação brasileira aplicável, em especial as certificações sobre segurança da informação solicitadas para Qualificação Técnico-Operacional, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.

5.1.9. A empresa contratada deve disponibilizar canais de atendimento para o registro e abertura de chamados, com no mínimo um canal de atendimento via WEB e um canal telefônico, do tipo 0800 junto ao fabricante da solução.

5.2. REQUISITOS DE SEGURANÇA

5.2.1. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pela CONTRATANTE, incluindo as Políticas e Diretrizes do Governo do Estado.

5.2.2. Prover criptografia de arquivos em repouso utilizando chave simétrica usando, no mínimo, algoritmo AES com 128 bits ou compatível.

5.2.3. Quando fornecido em nuvem, o fabricante deverá comprovar por meio de certificações reconhecidas no mercado e relatórios de auditoria independente, a segurança de seu ambiente data center.

5.2.4. Deverá disponibilizar, no mínimo, um ambiente não-produtivo de Desenvolvimento - DEV e um ambiente Produção, devendo possuir funcionalidades de desenvolvimento em ambiente de DEV e publicação em outros ambientes, com controle de versionamento e publicação.

5.2.5. Permitir a criação de campos compartilhados nos formulários da aplicação e que possam ser utilizados em quaisquer outras entidades, sem a necessidade de programação ou alteração do código-fonte.

5.2.6. Consolidar vários recursos de automação em um único ambiente para que os proprietários e desenvolvedores de processos possam construir e visualizar processos de negócios a partir de uma única interface.

5.2.7. Incluir fluxos e ações acionadas por eventos, como por exemplo itens do catálogo de serviço.

5.2.8. Consolidar as informações de configuração e tempo de execução em uma única interface para que os proprietários e desenvolvedores de processos possam criar, operar e solucionar problemas de fluxos a partir desta interface.

5.2.9. Permitir que sejam criados processos automatizados em um único ambiente utilizando linguagem natural para automatizar ações, tarefas, notificações e operações de registro sem codificação.

5.2.10. Fornecer descrições em linguagem natural da lógica de fluxo para ajudar usuários não técnicos a entender gatilhos, ações, entradas e saídas.

5.2.11. Promover a automação de processos, permitindo que técnicos no assunto desenvolvam e compartilhem ações reutilizáveis com designers de fluxo.

5.2.12. Fornecer uma biblioteca de ações reutilizáveis, reduzindo os custos de desenvolvimento de novos fluxos para o CONTRATANTE.

5.3. **GERENCIAMENTO DE USUÁRIOS E PERMISSÕES DE ACESSO**

5.3.1. Permitir atribuir a um usuário ou grupo de usuários específico, o acesso à abertura, modificação e fechamento de registros.

5.3.2. Permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal.

5.3.3. Permitir configurar a aprovação em fluxos de trabalho no mínimo com as seguintes regras para andamento do fluxo, sem necessidade de programação ou alterações do código-fonte:

I - Permitir aprovação por um usuário específico;

II - Permitir aprovação por conjuntos de usuários e regras específicas para sequência de aprovação;

III - Permitir aprovação pelo gerente de um grupo solucionador;

IV - Permitir aprovação pelo gerente do solicitante;

V - Permitir aprovação de acordo com o cargo e a estrutura de cargos da organização de forma recursiva (independentemente da quantidade de níveis ascendentes) e dinâmica (não atrelado à usuário específico);

VI - Permitir aprovação por quantidade definida de pessoas em um grupo de solução;

VII - Permitir aprovação por vários grupos de solução;

VIII - Permitir aprovação por grupos de solução juntamente com usuário específico.

5.3.4. Permitir a configuração, sem alteração de código-fonte, para aprovações que não se enquadram no subitem anterior;

5.3.5. Permitir atribuir a um usuário ou grupo de usuários específico, o acesso à abertura, modificação e fechamento de registros;

5.3.6. Permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal.

5.4. FUNCIONALIDADES DE APROVAÇÕES EM FLUXOS DE TRABALHO

5.4.1. Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte.

5.4.2. Permitir configurar aprovação em fluxos trabalho no mínimo com as seguintes regras para andamento do fluxo, sem necessidade de programação ou alterações do código-fonte.

5.4.3. Aprovação por um usuário específico.

5.4.4. Aprovação por conjuntos de usuários e regras específicas para sequência de aprovação.

5.4.5. Aprovação pelo gerente de um grupo solucionador.

5.4.6. Aprovação pelo gerente do solicitante.

5.4.7. Aprovação de acordo com o cargo e a estrutura de cargos da organização de forma recursiva (independentemente da quantidade de níveis ascendentes) e dinâmica (não atrelado à usuário específico).

5.4.8. Aprovação por quantidade definida de pessoas em um grupo de solução.

5.4.9. Aprovação por vários grupos de solução.

5.4.10. Aprovação por grupos de solução juntamente com usuário específico.

5.5. REQUISITOS DE PAINÉIS DE CONTROLE, GRÁFICOS E RELATÓRIOS

5.5.1. Deve oferecer formulários, painéis e relatórios inerentes aos processos de gerenciamento dos serviços disponíveis na solução que sejam usuais de mercado (conforme biblioteca ITIL v3 e outras referências similares) e *Out-of-the-Box* (OOTB), ou seja, prontos para uso sem qualquer configuração, customização ou modificação especial.

5.5.2. Permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código fonte.

5.5.3. Permitir a criação de painéis e dashboards com gráficos do tipo pizza, linha, colunas, barras, mapa de calor e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte.

5.5.4. Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e dashboards da solução, possibilitando a alteração de eixos, título do gráfico, legenda, escala, rótulos de dados, tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código fonte.

5.5.5. Permitir aos atendentes e solucionadores de chamados criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos de usuários ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução.

5.5.6. Suportar a definição de indicadores de desempenho (KPIs).

5.5.7. Prover visão da central de serviços em tempo real.

5.5.8. Permitir exportar ou agendar a exportação dos dashboards em formato PDF.

5.5.9. Permitir o detalhamento de informações contidas em gráficos de dashboards em gráficos detalhados.

5.5.10. Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards de gestão, ajustando o layout e conteúdo do painel de acordo com suas necessidades.

5.5.11. Permitir aos usuários a configuração de painéis e dashboards agrupados por assunto e independentes entre si.

5.5.12. Permitir o gerenciamento de permissões por usuários e grupos para acesso aos painéis e dashboards da solução.

5.5.13. Permitir ao usuário organizar seus painéis e dashboards com listas de registros de seu interesse, possibilitando a escolha de colunas, realização de filtros e ordenação da lista.

5.5.14. Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.

5.5.15. Permitir a cópia e a personalização dos objetos mencionados no item anterior de forma não programática (“codeless” ou “lowcode”).

5.5.16. Deve prover um mecanismo de desenvolvimento de formulários, painéis e relatórios básicos ou avançados, de forma gráfica, por meio de recursos de arrastar e soltar (drag and drop), para a inclusão dos campos escolhidos e separadores. Esta funcionalidade deverá ser do tipo WYSIWYG (What You See Is What You Get), ou seja, deverá permitir a visualização do resultado final durante o desenvolvimento do mesmo.

5.5.17. Permitir o desenvolvimento de painéis de controle (*dashboards*) capazes de apresentar relatórios e gráficos operacionais e gerenciais em tempo real, e de acordo com o papel do usuário.

5.5.18. Devem os painéis de controle ter capacidade de navegação (*drill down*) até o nível do registro de atendimento.

5.5.19. Deve prover recursos para explorar tendências, padrões, anomalias e correlações em dados, permitindo, ao usuário, realizar análises complexas (*slice and dice*), reorganizar dinamicamente (*pivot*), filtrar, fazer análises detalhadas (*drill-down*) e representar graficamente os dados, em tempo real.

5.5.20. Devem prover recursos que permitam o cálculo e exibição do tempo de resolução de diferentes alvos SLA - tempo de resposta e tempo de solução - e exibição de informações resumidas sobre a quebra do SLA em incidentes, problemas, mudanças e serviços.

5.5.21. Permitir a geração de relatórios com base em qualquer combinação dos atributos (campos) contidos no âmbito da infraestrutura de dados.

5.5.22. Permitir a produção de relatórios customizados avançados, integradamente a outros processos ITSM.

5.5.23. Permitir a geração de relatórios, no mínimo, nos seguintes formatos: Adobe Reader® (PDF), *Comma-separated values* (CSV), Microsoft Office e HTML.

5.5.24. Permitir a integração com, no mínimo, as seguintes fontes de dados: XML, CSV, Web Services SOAP, Web Services Rest e Bancos de Dados relacionais através de ODBC e JDBC.

5.5.25. Deve ser possível criar relatórios gerenciais específicos para uma ou mais unidades de negócios ou grupos de usuários.

5.5.26. Permitir a distribuição automatizada de relatórios diretamente por e-mail para destinatários únicos ou listas de distribuição.

5.5.27. Deve prover a emissão de relatórios comparativos entre os níveis de serviço acordados e os níveis de serviço efetivamente realizados.

5.5.28. Deve prover a emissão de gráficos gerenciais consolidados por período, contendo os KPIs.

5.5.29. Deve prover recursos para o Gerenciamento dos SLAs, contemplando um Dashboard para aferição dos objetivos de níveis de serviço.

5.5.30. Permitir a geração, no mínimo, de relatórios tais como os listados a seguir: Relatório de serviços registrados no Catálogo de Serviços, com indicadores de número de serviços em transição, em produção e total.

5.6. **BASE DE CONHECIMENTO**

5.6.1. Possuir uma base de dados para armazenamento de artigos de conhecimento da organização.

5.6.2. Permitir configurar e gerenciar o ciclo de vida de registros de artigos de conhecimento.

5.6.3. Possuir recurso para busca indexada, apresentando soluções para os atendentes.

5.6.4. Permitir classificar e atribuir categorias para os artigos de conhecimento.

5.6.5. Permitir a pesquisa de artigos de conhecimento nas telas de atendimento de registros dos processos de gerenciamento de incidente, mudança, problema, requisições.

5.6.6. Possuir campos de pesquisa de conhecimento, integrados com a base de conhecimento da solução, nas interfaces de solicitação e operação de aplicações, processos e fluxos de trabalho do CONTRATANTE.

5.6.7. Permitir gerenciar documentos de conhecimento estabelecendo prazos de validade e de revisão.

5.6.8. Permitir o gerenciamento de acesso de usuários aos artigos de conhecimento.

5.6.9. Permitir inserir ou anexar imagens, vídeos e textos artigos de conhecimento.

5.6.10. Permitir pesquisar através de palavras-chave ou frases inteiras.

5.6.11. Permitir controlar o processo de aprovação de um documento, antes do mesmo ser publicado na base de conhecimento.

5.6.12. Permitir o ranking de uso das informações de conhecimento e identificar as necessidades não atendidas por conhecimento, de forma que o próprio usuário final possa classificar a utilidade (ou não) do artigo de conhecimento.

5.6.13. Deve permitir o cadastro, alteração, revisão, desativação, publicação de procedimentos para a base de conhecimento (perguntas frequentes, erros conhecidos, soluções de contorno, entre outros.) e o público para o qual deve ser disponibilizado (equipes de TI, usuários finais, etc.), de forma que incidentes e problemas já diagnosticados ou resolvidos possam ser registrados e pesquisados para facilitar e aumentar a velocidade de solução de futuras ocorrências.

5.6.14. Deve integrar nativamente o processo de Gerenciamento de Conhecimento aos processos de Gerenciamento de Incidentes, Gerenciamento de Problemas e Gerenciamento de Configurações.

5.6.15. Permitir o recebimento de propostas de ativos de conhecimento, sua posterior análise e sua aceitação ou rejeição. Esse recebimento de propostas deve ter origem no Gerenciamento de Incidentes, no Gerenciamento de Problemas, no Gerenciamento de Configuração ou em uma solicitação direta de um usuário.

5.6.16. Deve permitir revisões para cada ativo de conhecimento.

5.6.17. Deve implementar recursos comuns de gerenciamento de documentos, incluindo: captura, classificação, marcação e indexação, pesquisa e recuperação, controle de versão, segurança e gerenciamento de acesso.

5.6.18. Deve permitir a estruturação do conteúdo da KB (Knowledge Base) na forma "Wiki", sem depender de codificação.

5.6.19. Deve fornecer uma plataforma de gerenciamento de KB (Knowledge Base) exclusiva para todos os usuários de diferentes equipes e departamentos.

5.6.20. Deve controlar as permissões de acesso à plataforma KB (Knowledge Base) com base em papeis, equipe do usuário ou com base em grupos.

5.6.21. Deve obter automaticamente itens relevantes da base de conhecimento com base nas pesquisas dos usuários ou contextualmente, para resolução de incidentes de autoatendimento

5.6.22. Deve oferecer funcionalidade semelhante blogs para permitir a pesquisa, postagem e acompanhamento de tópicos de resolução de problemas.

5.6.23. Permitir uma variedade de mídias, incluindo arquivos de áudio e vídeo internos ou externos (por exemplo, vídeos do YouTube), links, arquivos, etc.

5.6.24. Deve fornecer recursos de colaboração social, incluindo: perfis e funções dos usuários, postagens dos usuários, curtidas e comentários, bate-papos e mensagens (internos à solução).

5.6.25. Possuir uma interface fácil e iterativa para a consulta a base de conhecimento, tanto para o analista quanto para o usuário final.

5.6.26. Possuir a integração nativa do Gerenciamento do Conhecimento com os demais processos (nativos da solução ou implementados para atendimento de processos de trabalho), permitindo, por exemplo, mas não limitado a tal, a associação de documentos e artigos de conhecimento a eventos, incidentes, problemas, mudanças e registros de fluxos de trabalho automatizados na solução.

5.6.27. Possuir recursos de pesquisa de soluções aos usuários enquanto registram as solicitações.

5.6.28. Rastrear, automaticamente, quantas vezes um artigo ou informação de conhecimento foi utilizado.

5.6.29. Deve possuir uma base de conhecimento onde serão registradas soluções para os problemas e erros conhecidos, possibilitando relacionar os problemas e suas respectivas soluções a mudanças e a incidentes específicos.

5.6.30. Permitir consulta rápida, por palavras-chave, das informações que se encontram na base de conhecimento e possibilitar a navegação na hierarquia de tópicos ou assuntos.

5.6.31. Deve possibilitar, aos usuários administrativos, ou outros usuários, com nível de autorização suficiente, o gerenciamento (inclusão, alteração, consulta e exclusão) das informações armazenadas na base de conhecimento.

5.7. RELACIONAMENTO DE REGISTROS

5.7.1. Possuir interface de lista de registros de qualquer processo ou fluxo de trabalho da solução, seja nativo ou criado para o CONTRATANTE, totalmente customizável, permitindo adicionar, remover ou alterar a ordem das colunas no grid de visualização de registros.

5.7.2. Permitir filtros e consultas a partir de qualquer coluna listada no grid de registros.

5.7.3. Permitir que usuários refinem a pesquisa com consultas avançadas, podendo inserir vários critérios de consulta e filtros no grid de registros.

5.7.4. Permitir que consultas personalizadas possam ser gravadas e compartilhadas com outros usuários da solução.

5.7.5. Permitir aos usuários inserir e remover quantas colunas forem necessárias em sua lista e grids, desde que estas estejam na tabela de banco de dados ao qual estão sendo listados os registros.

5.7.6. Permitir a alteração da ordem de apresentação das colunas no grid de registros.

5.7.7. Permitir ordenar a lista de registros por qualquer das colunas do grid de visualização, de A a Z e de maior para menor, ou vice-versa.

5.7.8. Permitir atualizar manualmente as consultas exibidas nas listas e grids (refresh) sem fechar ou atualizar toda a janela atual do navegador.

5.7.9. Permitir que usuários salvem seus filtros / pesquisas.

5.7.10. Permitir que usuários compartilhem os filtros entre usuários e grupos.

5.7.11. Permitir que usuários realizem pesquisas e filtros avançados.

5.7.12. Permitir que os usuários exportem para arquivos formato Excel, CSV e XML.

5.7.13. Permitir que usuários importem dados para criação e alteração de registros com base em modelo no formato Excel, CSV e XML.

5.7.14. A personalização de listas e grids não devem depender de um usuário administrador, sendo facultado a qualquer outro operador a criação de suas próprias listas e grids, não estando restrito às listas e grids originalmente disponíveis na aplicação ou disponibilizadas pelos administradores.

5.7.15. Permitir a alteração de registros, inclusive alterações em lote (vários registros), na própria tela de visualização de registros e grid da solução.

5.7.16. A solução deve possuir recurso que permita aos operadores fazer a listagem de todos os registros em sua fila ou fila de grupos de solução a que pertence, combinando registros de incidentes, requisições, mudanças e tarefas de processos e fluxos de trabalho.

5.7.17. Permitir a criação de novos registros ou exclusão de registros, a par da lista de registros.

5.7.18. Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte.

5.7.19. Permitir o relacionamento de tabelas de bancos de dados criadas para automação de aplicações, processos e fluxos de trabalho do CONTRATANTE, com tabelas e bancos de dados nativos da solução, sem a necessidade de programação ou alterações do código-fonte

5.8. **MANIPULAÇÃO DE DADOS E FORMULÁRIOS EXISTENTES E/OU NOVOS**

5.8.1. Possuir recursos gráficos de workflow interativos para criação de processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos fluxos de trabalho.

5.8.2. Apresentar componente próprio para a modelagem gráfica e a automação de processos e fluxos de trabalho na solução.

5.8.3. Permitir a criação dessas aplicações sem uso de código, para que toda a empresa possa desenvolver e u lizar novas aplicações integradas a plataforma.

5.8.4. Possuir um Estúdio IDE Integrado para desenvolvimento de aplicações integradas a plataforma.

5.8.5. O IDE deve possuir wizard que automaticamente crie as aplicações web e para o aplicativo mobile.

5.8.6. As novas aplicações deverão gerar tabelas independentes das outras aplicações. Isto é, independente de outros módulos da solução.

5.8.7. Uma nova aplicação deverá conter no mínimo:

I - Tabelas;

II - Elementos gráficos de interface do usuário: Menus, Módulos, Listas e Formulários;

III - Arquivos da Aplicação: Regras de Negócio, Workflows, Ações gráficas (UIs);

IV - Integrações: Rest Web Services, JSON Data Format, SOAP, e outras possíveis integrações dessa aplicação;

V - Dependências: Tabelas de tarefas, Gerenciamento de SLA, Base de Usuários e seus respectivos acessos;

VI - Permitir a construção independente, de menus, telas, módulos para a mesma aplicação em dispositivo móvel (iOS e Android) em aplicativo fornecido nativamente pela solução;

VII - Integrar com gerenciador de controle de versões de código fontes (GIT).

5.8.8. Permitir que os desenvolvedores de aplicativos se integrem a um repositório de controle de origem (GIT), salve e gerencie várias versões de um aplicativo em ambiente desenvolvimento e/ou homologação.

5.8.9. O sistema deve gerar um arquivo controle de integridade (*checksum*) no repositório GIT para determinar se algum arquivo do aplicativo foi alterado fora da IDE de desenvolvimento. Como exemplo de rotina de integração desejada, espera-se que quando o valor da soma de verificação do arquivo corresponde ao valor da soma de verificação atual, a integração ignora o processo de validação e sanitização. Quando os valores da soma de verificação não correspondem, a integração valida e limpa os arquivos do aplicativo como parte da operação de controle de origem.

5.8.10. Permitir a automação de fluxos de trabalho de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código-fonte.

5.8.11. Possuir ferramenta de criação de formulários com campos específicos de cada processo e fluxo de trabalho, a fim de personalizar a inserção de informações e controles de acordo com a necessidade do CONTRATANTE, sem a necessidade de programação ou alteração do código-fonte.

5.8.12. Dispensar a necessidade a criação, de forma manual (usando scripts e programação), de tabelas, colunas e campos de banco de dados na solução, tornando estas atividades, quando necessárias, transparentes aos administradores da solução.

5.8.13. Permitir a customização de menus, formulários, *labels*, de automações de fluxos de trabalho e processos do CONTRATANTE, desenvolvidos e implementados na solução, permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código fonte.

5.8.14. Permitir a configuração de ciclos de vida específicos para fluxos de trabalho ou processo automatizados na solução.

5.8.15. Permitir que os processos e fluxos de trabalho automatizados na solução possuam as mesmas funcionalidades nativas disponibilizadas na solução, como por exemplo: requisitos de usabilidade da lista de registros, citados nesta especificação técnica, ferramentas de colaboração como chat e notificações, permitindo comunicação entre usuários e provedor de serviços, personalização de menus, regras de aprovação de fluxos, relacionamento entre processos, painéis e dashboards automatizados.

5.8.16. Deve possuir o conceito de segregação de aplicações, escopo de aplicações, funções dentro do escopo só poderão ser acessadas ou manipuladas por aqueles que possuem acesso. (Exemplo: Escopo de aplicações do Dpto. Jurídico, Escopo de Aplicações do RH etc.)

5.8.17. Possuir o conceito de hierarquia de escopo de aplicações.

5.8.18. Possuir controle de dependências entre aplicações e privilégios de acesso.

5.8.19. Permitir o compartilhamento de aplicações entre outras instâncias, sejam de desenvolvimento, teste ou em produção.

5.8.20. Possuir mecanismo de teste automatizado de versões de aplicações, dentro da própria solução, o qual permite criar e executar testes automatizados para confirmar se a instância funciona após fazer uma alteração. Por exemplo, após uma atualização, durante o desenvolvimento do aplicativo ou ao implementar configurações de instância com conjuntos de atualização, o mecanismo deverá revisar os resultados do teste que apresentaram falha, identificando as mudanças que causaram a falha e devem ser revisadas.

5.8.21. Permitir que sejam criados vários testes e fiquem disponíveis para futuros testes de upgrade ou mudanças nas aplicações, podendo ser reutilizados, permitindo pelo menos os seguintes testes:

I - Testar operações básicas de um formulário;

II - Fazer referência a um valor de uma etapa anterior em um workflow. (Exemplo: Testar atribuição a um campo de formulário do valor de uma variável de saída de uma etapa anterior);

III - Testar uma regra de negócio que deva ser aplicado em alguma etapa;

IV - Testar o workflow de um processo.

5.8.22. Após a configuração de uma aplicação permitir visualizar como a aplicação funcionaria no Tablet, em um computador ou em um dispositivo celular.

5.8.23. Permitir que possa utilizar/estender as tabelas de uma determinada aplicação para criar outras aplicações.

5.8.24. Permitir a comunicação em tempo real entre usuários, usuários e atendentes dos serviços.

5.8.25. Incluir anotações nos registros da solução, possibilitando aos operadores atendentes publicar e tornar visível ou não para os usuários.

5.8.26. Registrar toda comunicação entre usuários e atendentes dos serviços nos registros da plataforma.

5.8.27. Permitir comunicação entre as partes interessadas e envolvidas nos processos e em atendimentos dos serviços, onde a plataforma deve possibilitar a inserção de notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados.

5.8.28. Configurar as notificações automáticas de alertas para reiterar chamados técnicos abertos.

5.8.29. Enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementado na solução.

5.8.30. Enviar notificações baseadas em condições e eventos da solução.

5.9. **GESTÃO DE ATENDIMENTO**

5.10. A solução deve possuir em sua plataforma uma aplicação de Gerenciamento de Serviços a Clientes internos e externos do CONTRATANTE, a qual possui como foco atender aos usuários de uma forma avançada e com qualidade. Neste ponto, a solução deve:

5.11. Possuir funcionalidade que permita construir (customizar) de forma no code/low code portais customizados por tipo de cliente ou cidadão;

5.12. Possuir um modelo de dados centralizado e integrado baseado em nuvem com CMDB nativo;

5.13. Permitir suporte para desenvolvedores no-code, low-code e pro-code;

5.14. Possuir ambiente, permitindo que os atendentes do telefone, o portal, o chat e a interação por e-mail sejam feitos pela mesma aplicação;

5.15. Permitir automatizar tarefas redundantes para o cliente, por meio do Chatbot;

5.16. Possuir regras de roteamento sofisticado, utilizando regras baseado em perfil do agente e da solicitação, geografia do agente, compromisso contratual, disponibilidade do agente, carga de trabalho do agente e outras prioridades customizáveis;

5.17. Possuir a funcionalidade de forçar perfis mandatório para atendimento de casos que exigem esse tipo de perfil profissional;

5.18. Possuir funcionalidade de Inteligência Artificial, Machine Learning para automaticamente assinalar quem irá atender, categorizar e priorizar automaticamente. Essa inteligência deve aprender baseada nos dados históricos;

5.19. Fornecer alertas aos agentes e fazer a linha de tempo de interação com o cliente/solicitante;

5.20. Deve ter uma camada de colaboração avançada para suportar as comunicações da equipe;

5.21. Deve fornecer notificações proativas de suporte via e-mail, SMS e portal para os clientes afetados;

5.22. Deve ter um recurso de serviço de atendimento em campo totalmente integrado na mesma plataforma, por meio de aplicativo móvel, que deve funcionar on-line e off-line para atividades, permitindo a sincronização quando estiver conectado;

5.23. Deve fornecer autoatendimento personalizado por meio de um portal de serviços configurável que incorpora uma base de conhecimento, catálogo de serviços e comunidades;

5.24. Deve ser capaz de conectar outros departamentos aos processos de atendimento ao cliente em uma única plataforma com aderência interna aos níveis mínimos de serviços;

5.25. Deve ser capaz de suportar diferentes SLA's para diferentes produtos pertencentes a um cliente;

5.26. Permitir SLA's para objetos diferentes do objeto "caso", como em tarefas, incidentes, problemas, alterações e solicitações associados a um caso;

5.27. Deve fornecer gerenciamento de solicitações com várias camadas e permitir o relacionamento com registros de incidente, problemas e outras solicitações de serviço;

5.28. Deve fornecer escalonamento automático sem intervenção manual;

5.29. Deve fornecer chatbot ou agente virtual que permita o desenvolvimento de diálogos conversacionais;

5.30. Deve fornecer um espaço de trabalho eficiente do agente que permita que os agentes executem várias tarefas no trabalho em vários canais, como telefone, bate-papo, e-mail e web;

5.31. O espaço de trabalho do agente deve exibir informações contextuais automaticamente para oferecer suporte à resolução rápida de casos. Isso inclui artigos de conhecimento contextualizado, publicações na comunidade e itens de catálogo de serviços. Os agentes devem poder anexar artigos aos casos;

5.32. A solução deve permitir o feedback do cliente sobre o artigo da base de conhecimento, por meio de um processo estruturado e automatizado de feedback;

5.33. Permitir que os agentes sinalizem quando algo está faltando no artigo da base de conhecimento e isso deve alimentar o processo de feedback estruturado de ajuste da base de conhecimento;

5.34. Na gestão do conhecimento, a solução deve permitir a definição de blocos de conteúdo reutilizáveis que possam ser incorporados em vários artigos de conhecimento, a fim de reduzir a redundância. Os blocos de conhecimento devem poder ser restringidos pelo papel do usuário.

6. SERVIÇO DE TREINAMENTO DAS SOLUÇÕES

6.1. Os serviços de treinamento deverão ocorrer em até 15 dias após a emissão da O.S. (Ordem de Serviço) e consiste em realizar o adequado repasse de conhecimentos para as equipes técnicas que virão a operar os softwares.

6.2. Os treinamentos deverão abordar, minimamente, demonstração de todos os componentes da solução contratada, orientando sua correta utilização e funcionamento, bem como orientando à cerca da configuração, utilização e administração dos recursos.

6.3. Os treinamentos deverão ter duração mínima de 40 (quarenta) horas sendo no mínimo 8 (oito) horas para cada solução fornecida e o tempo restante dedicado à realização de exercícios práticos que permitam que os participantes operem a solução e testem o conhecimento adquirido na prática.

6.4. Os treinantos deverão ser quantificados por aluno, sendo pemitido que e a Contratada reúna na mesma turma alunos de Órgãos diferentes. Uma turma deverá ser formada por no máximo 16 alunos.

6.5. Uma vez que o treinamento ocorra online, este deverá ser gravado e disponibilizado ao CONTRATANTE.

6.6. Todos os treinamentos deverão ocorrer com aulas ao vivo, independente da modalidade escolhida.

6.7. O material didático deverá ser fornecido em meio digital pela CONTRATADA até 5 (cinco) dias antes do início das aulas, para que seja disponibilizado para seus participantes.

6.8. A CONTRATADA deverá registrar a presença dos alunos e, ao final do treinamento, emitir certificado de participação para cada um dos participantes que tiver participado de no mínimo, 70% (setenta por cento) das aulas.

6.9. O material didático, lista dos participantes com controle de frequência bem como a gravação do treinamento são evidências necessárias para fins de comprovação da conclusão das atividades e pagamento.

6.10. Ao final do treinamento, deverá ser preenchida por cada um dos participantes, ficha de avaliação do treinamento pontuando de 0 a 10 cada um dos critérios abaixo, para cada uma das Soluções:

a) Didática do instrutor;

b) Conteúdo apresentado;

c) Exercícios práticos;

d) Avaliação geral.

6.11. Para cada turma de treinamento, a nota final calculada pela média aritmética das avaliações, não poderá ser inferior a 70%. Caso a nota seja inferior, caberá a CONTRATADA mapear junto a CONTRATANTE os pontos fracos para que seja ministrada aula de reforço de 4 (quatro) horas para cada ponto onde o reforço se faça necessário.

7. SERVIÇO TÉCNICO DE APOIO NA IMPLANTAÇÃO DAS SOLUÇÕES E ADEQUAÇÃO À LGPD

7.1. A CONTRATANTE autorizará os serviços mediante emissão de Ordem de Serviço (OS) à CONTRATADA, elaborada conforme ANEXO III – Modelo de Ordem de Serviço, onde os serviços serão mensurados com base na quantidade de UST necessária a execução de cada atividade.

7.2. A quantidade de UST para uma atividade será definido com base no esforço em horas necessário ao alcance dos resultados pretendidos e elaboração dos produtos.

7.3. Os serviços deverão estar vinculados a entrega de produtos e resultados que possam ser aferidos e atestados pela CONTRATANTE, não devendo em hipótese alguma serem contratadas horas ou UST que não estejam vinculadas a resultados ou produtos que possam ser avaliados quanto aos níveis mínimos de serviço apresentados neste Termo de Referência.

7.4. Ainda que tratem de atividades continuadas executadas mensalmente, caberá a CONTRATANTE e CONTRATADA definir previamente as atividades que serão executadas bem como resultados e produtos que serão entregues ao final de cada ciclo.

7.5. Quando se tratar de resultados que não possam estar diretamente vinculados a um produto, caberá a CONTRATADA apresentar um Relatório Técnico de Atividades - RTA relacionando as atividades executadas e evidências de sua execução, para fins de ateste dos serviços.

7.6. Uma vez emitida a ordem de serviço, a mesma só poderá ter seu escopo alterado por meio da formalização de aditivo apresentando as justificativas para as mudanças que vierem ocorrer, devendo as justificativas serem apresentadas pela parte que motivar as mudanças.

7.7. As Ordens de Serviço deverão ser precedidas de Proposta Técnica, a ser elaborada pela CONTRATADA por solicitação da CONTRATANTE, que deverá conter no mínimo:

a) Documento de Especificação do Projeto;

b) Relação das atividades e esforço em horas;

c) Cronograma estimado;

d) Entregáveis e custo total.

7.8. O pagamento dos serviços ocorrerá quando do recebimento definitivo dos produtos que compõe a Ordem de Serviço.

7.9. Desde que haja anuência da CONTRATANTE, os produtos e serviços de uma Ordem de Serviço poderão ser pagos separadamente, desde que os produtos que tenham sido entregues sejam produtos independentes de outros produtos ou serviços da mesma Ordem de Serviço.

7.10. CATÁLOGO DE SERVIÇOS

7.10.1. Para mensuração da quantidade de UST necessária para execução dos serviços, foi desenvolvido um Catálogo de Serviços relacionando as atividades necessárias e previstas para entrega do objeto, a necessidade / justificativa e as métricas para quantificação dos volumes de serviços necessários para alcance dos objetivos, apresentado na tabela abaixo.

7.10.2. As atividades do Catálogo de Serviço representam mera expectativa, sendo admitida a execução de outras atividades que venham a ser necessárias, limitadas ao total de UST que venha a ser contratado.

7.10.3. Os serviços constantes do Catálogo de Serviços, quando necessário, devem contemplar orientações acerca dos cuidados a serem tomados também com dados físicos que possam estar sob guarda do órgão contratante.

7.10.4. O Catálogo de Serviços Técnicos de Apoio no Diagnóstico e Adequação à LGPD e Operação das Soluções, contendo lista de serviços, descrições, aplicações, entregáveis e mensurações, consta do Anexo II deste Termo de Referência.

7.10.5. Tecnologias

7.10.5.1. Para realização dos serviços de Análise de Segurança em ativos tecnológicos e aplicações, itens 4 e 5 do catálogo do serviço, deverão ser empregadas tecnologias para a realização de varreduras automatizadas para descoberta de vulnerabilidades ou fragilidades de segurança, onde para tanto as tecnologias deverão ser dotadas dos seguintes recursos:

I - **Para Vulnerabilidades em Ativos Tecnológicos**

a) O software utilizado nesse serviço deverá realizar análise de vulnerabilidades, classificações de risco cibernético ou priorização bem como permitir o encaminhamento das vulnerabilidades aos responsáveis pelo tratamento dando suporte para equipes de segurança da informação no processo de tratamento, com informações, priorização e recomendações baseado na probabilidade e na criticidade da vulnerabilidade, analisando vulnerabilidades presentes na National Vulnerability Database (NVD), para subsidiar e apoiar a correção e configuração de controles de compensação.

b) A ferramenta deve funcionar sem a necessidade de agentes instalados nos ativos que serão alvo de análise de vulnerabilidade, onde a base de vulnerabilidades conhecidas deve ser atualizada automaticamente durante a prestação dos serviços sem intervenção do administrador, sendo capaz de identificar no mínimo 50.000 CVE (Common Vulnerabilities and Expossures), utilizando CVE associados às vulnerabilidades identificadas para geração de relatórios, gerenciamento de riscos e mitigação de ameaças, realizando a associação dos riscos as vulnerabilidades identificadas.

Obs: O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo o CVSS v3 Impact Score, a idade da vulnerabilidade e o número de produtos afetados pela vulnerabilidade;

c) Deverá possuir sistema de criação de Ticket no sistema de chamados interno da solução.

d) Deverá ser capaz de identificar os hosts no ambiente sem a necessidade de execução manual de uma varredura pelo administrador (discovery automático).

e) Deverá permitir a configuração de políticas de varreduras diferentes a serem aplicadas a grupos de servidores específicos.

f) A ferramenta deve possuir sistema para a sinalização de falsos positivos e controle de acesso baseado em perfis de usuário, com mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência.

g) Deverá ser capaz de verificar vulnerabilidades em gerenciadores de virtualização como Hyper-V e VMware bem como possuir em sua base de vulnerabilidades, para cada item cadastrado, no mínimo as seguintes informações: nome, descrição, nível de risco, score CVSS BASE, TEMPORAL e ENVIRONMENTAL, referência (CVE, CWE, BugTraq ou outra fonte), solução e link para o download da correção e contramedidas, quando aplicável, informação e fonte de exploit.

h) A solução deve permitir o cadastramento de credenciais utilizadas para escaneamento para que seja permitido o uso de tais credenciais para futuros escaneamentos, sem que o administrador da ferramenta saiba a senha destas credenciais.

II - **Para Vulnerabilidades em Aplicações**

a) Deve possuir mecanismos para análises de vulnerabilidades SAST (Análise Estática da segurança do código-fonte de aplicações web), DAST (Análise Dinâmica da segurança de aplicações web com mapeamento profundo e injeção de dados) e MAST (Análise Estática da segurança do código-fonte de aplicações móveis (Android e iOS)), realizando varreduras com métodos baseados em documentos abertos, contemplando no mínimo o Top 10 OWASP (Open Web Application Security Project), Top 25 CWE (Common Weakness Enumeration), Top 5 PHP (baseado no OWASP PHP Top 5) Injeção de Falhas (focado em falhas de injeção de dados, tais como XSS, Injeção de SQL, Inclusão de Arquivos e Execução de Comandos), Força-Bruta de Estrutura (focado em descobrir arquivos comuns de backup, páginas administrativas e exposições similares), Arquivos de Backup (em arquivos de backup, ocultos e obsoletos, mas não tão agressivamente quanto o método Força-Bruta de Estrutura), teste completo de penetração, SQL Injection, XSS (vulnerabilidades de Cross-Site Scripting (XSS) e evasão de filtros anti-XSS), inclusão de arquivos (focado em vulnerabilidades de inclusão de arquivo local ou remoto, Conteúdo Malicioso (focado em malware, backdoors, pontos de entrada ocultos e sinais de invasão), Redirecionamentos Não Validados (focado em vulnerabilidades em redirecionamentos), Scan de Aplicação no Lado Servidor (focado apenas em vulnerabilidades no lado do servidor através de análise dinâmica ou de código-fonte).

b) Deve possuir conformidade com o padrão CVSS (Common Vulnerability Scoring system) versão 2.0 e 3.0, para comunicar a gravidade de uma vulnerabilidade e ajudar a determinar a urgência e prioridade da resposta de segurança, incluindo os seguintes cálculos:

b1) Pontuação Base;

b2) Pontuação Temporal;

b3) Pontuação de Exploração;

b4) Pontuação de Impacto.

III - **Quanto à análise de código-fonte**

a) Deve suportar códigos embutidos em HTML e formas abreviadas de print.

b) Deve ser capaz de identificar vulnerabilidades no lado do cliente ou no lado do servidor (client-side e server-side).

c) Deve ser capaz de realizar a análise de vulnerabilidades sobre códigos-fonte completos, trechos de código-fonte e arquivos de configuração.

d) Deve ser capaz de identificar em aplicações móveis os seguintes riscos que fazem parte do documento Mobile Top 10 elaborado pelo projeto de código aberto OWASP (Open Web Application Security Project):

d1) Uso Inadequado da Plataforma;

d2) Armazenamento Inseguro de Dados;

d3) Comunicação Insegura;

d4) Autenticação Insegura;

d5) Criptografia Insuficiente;

d6) Autorização Insegura;

d7) Qualidade do Código do Cliente;

d8) Adulteração de Código;

d9) Engenharia Reversa;

d10) Funcionalidade Estranha.

IV - **Quanto à análise dinâmica**

a) Deve detectar vulnerabilidades de segurança em aplicações web dinâmicas e servidores web, mapeando a estrutura, incluindo todos os links e pontos de entrada de dados da aplicação alvo, no mínimo através das seguintes técnicas de análise de código HTML, reconhecimento e preenchimento automático de formulários, seguimento de redirecionamentos, análise e execução de código JavaScrip e chamadas XHR, análise do arquivo robots.txt de um website, se houver.

b) Deve ser capaz de realizar injeções de dados e manipular parâmetros na aplicação alvo em URLs e formulários (GET e POST).

c) Deve ser capaz de realizar mutações na injeção de dados em aplicações, de modo a abranger todas as linguagens de programação e plataformas alvo suportadas pela solução.

d) Deve ser capaz de identificar vulnerabilidades no lado do cliente ou no lado do servidor (client-side e server-side).

e) Deve ser capaz de identificar vulnerabilidades como injeção de SQL, injeção de NoSQL, injeção de comando, exposição e injeção de código.

f) Deve ser capaz de identificar softwares desatualizados e vulneráveis.

g) Deve ser capaz de realizar ataques de força-bruta estrutural e de autenticação: HTTP e em formulários de login de maneira automática

h) Deve ser otimizado para testar aplicações rodando nos seguintes servidores HTTP: Apache, Apache Tomcat, Microsoft IIS, Nginx.

V - **Funcionalidades técnicas de análise**

a) Deve permitir a identificação dos seguintes tipos de vulnerabilidade e exposições em aplicações web, bem como em aplicações móveis sempre que aplicável: Abuso & Uso Indevido de API, aleatoriedade Insegura, algoritmos criptográficos e de Hash Inseguros, armazenamento inseguro de dados (casos de proteção de dados ausentes ou

insuficientes), autenticação quebrada, backdoor baseada na Web, arquivos e pastas comuns de Backup e Backup com Extensão Comum ou Dupla, cabeçalhos de segurança HTTP ausentes ou fracos, comentários suspeitos em Código-Fonte e HTML, comunicação insegura, configuração incorreta de segurança, conteúdo inapropriado ou malicioso, conteúdo padrão, criptografia quebrada, Cross-Site Scripting (XSS) (incluindo XSS baseado em DOM, específico para HTML5, filtro fraco de XSS e Cross Frame Scripting (XFS)), Directory Traversal, estouro de Buffer; execução de comando, exposição (caminho, código-Fonte, Banco de Dados, senha, endereço IP interno, tecnologia Web e outros), falsificação de Registro (Log), Solicitação Entre Sites e Solicitação do Lado do Servidor (SSRF), fraquezas comuns em Formulários (incluindo sequestro de formulário de e-mail, preenchimento automático ativado e transação de cartão de crédito não criptografada), hashing de senha fraco, inclusão de arquivo local ou remoto, injeção de cabeçalho HTTP, Divisão de resposta HTTP, injeção de Código (Expression Language e Expressão Regular); injeção (JSON, XML, XPath, XXE (XML External Entity), LDAP, NoSQL, SQL, HQL, SSI (Server-Side Includes)), informações confidenciais codificadas ou registradas, informações sensíveis do lado do cliente, listagem de diretório, login Não Criptografado, manipulação arbitrária de arquivos, manipulação de Cookies, más práticas, métodos perigosos, negação-de-serviço (DoS) no lado do cliente e servidor, pontos de entrada de depuração (incluindo parâmetros de depuração ocultos), protocolos fracos, redirecionamentos não validado, salting inseguro, string de formato não controlada, vazamento de informações ou uso de armazenamento local, bem como dados confidenciais guardados no armazenamento local.

7.10.5.2. A Licitante deverá indicar em sua proposta o(s) software(s) que virá(ão) ser empregado(s) na execução dos serviços, devendo mantê-lo(s) disponível(eis) para a realização de reteste por um período de no mínimo 90 (noventa) dias, necessário para o tratamento das vulnerabilidades identificadas.

8. EQUIPE DE PLANEJAMENTO

Manuelito de Sousa Reis Junior Gerente de Riscos e Ameaças Id Funcional: 4406953-7	Sâmya Massari Lima Encarregada de Dados Pessoais Id Funcional: 5108516-0

Rio de Janeiro, 20 de abril de 2023.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/04/2023, às 00:29, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Sâmya Massari Lima**, **Diretora**, em 24/04/2023, às 11:50, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **49852091** e o código CRC **7BAFE5F6**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO II DO TERMO DE REFERÊNCIA

CATÁLOGO DE SERVIÇOS

ITEM	SERVIÇO	NECESSIDADE / JUSTIFICATIVA	DETALHAMENTO	ENTREGÁVEIS	UNIDADE	QUANTIDADE DE UST POR UNIDADE
1	Serviço de integração e customização das Soluções	Para o bom funcionamento das estratégias de conformidade com a LGPD, se faz necessário que cada uma das soluções seja corretamente implantada, estabelecendo processos e automatizando ao máximo o levantamento de informações e os fluxos para tratamento das demandas necessárias ao funcionamento destas estratégias.	Os serviços de implantação consistem na customização, parametrizações, configurações das Soluções às especificidades do ambiente de cada órgão que vier a contratá-las, contemplando entre outros a criação de formulários customizados, gráficos e relatórios e principalmente integrações necessárias ao perfeito funcionamento das Soluções, onde os serviços serão demandados com base na quantidade de Soluções adquiridas e a quantidade de UST definida com base no planejamento proposto e aprovado.	- Relatório contendo relação das tarefas executadas, registros das configurações executadas e integrações realizadas	solução contratada	2.000
2	Serviço de Diagnóstico e Mapeamento de Dados	Para cada área onde é realizado o tratamento de dados, se faz necessário o mapeamento dos processos que realizam tratamento de dados para que seja possível conhecer todas as etapas envolvidas em seu tratamento. A partir desse conhecimento, será possível avaliar esses processos e identificar riscos e identificar as adequações necessárias à conformidade com a LGPD.	O serviço em questão é voltado ao diagnóstico e mapeamento dos processos que envolvem o tratamento de dados pessoais, contemplando a estruturação dos dados na Solução para gestão da privacidade e serão executados tendo como referência a quantidade de áreas que virão a ter seus processos de tratamento de dados mapeados.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Resultado da Avaliação de maturidade realizada; - Inventário dos processos identificados que tratam dados pessoais bem como seus fluxos operacionais de forma gráfica; - Registro de todas as Operações de Tratamento de Dados identificadas durante a etapa de mapeamento/inventário; - Relatórios Técnicos gerados a partir das avaliações das minutas contratuais e normativos internos; - Resultado do Gap Analysis da ISO 27001 e 27701; - Lista das ações e controles necessários a Implementação de estratégias de Privacidade; - Plano de ação.	área entrevistada	16
3	Serviço de Descoberta de Dados	A realização da descoberta de dados pessoais em fontes de dados estruturados (instância de bancos de dados) e não-estruturadas apoiará no mapeamento dos dados e na automatização dos processos de requisições de titulares bem como na criação de fluxos inteligentes de respostas às requisições, além de permitir maior governança e proteção dos dados tratados no âmbito do órgão, em especial os dados pessoais.	O serviço em questão é voltado a consolidação dos resultados e apresentação dos mesmos em forma de relatório bem como a realização de carga e validação dos dados na Solução de LGPD.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Resultado das descobertas de dados; e - Catálogo dos dados gerado a partir da descoberta dos dados pessoais validados.	bloco de instâncias de banco de dados ou fontes de dados	16
4	Serviço de Análise de Segurança para descoberta de vulnerabilidades em ativos tecnológicos	A análise de segurança para identificação de vulnerabilidades em ativos tecnológicos é fundamental para atendimento a Lei, em especial no que diz respeito ao Art. 6, inciso VII que prevê a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados.	O serviço em questão prevê o emprego de tecnologia para realizar de forma automatizada a varredura para descoberta de vulnerabilidades na infraestrutura tecnológica da contratante de modo que seja possível indicar e tratar aquelas que ofereçam maior risco de acessos não autorizados no ambiente ou que possam comprometer a segurança.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Resumo executivo das vulnerabilidades encontradas; - Relação dos ativos tecnológicos analisados; - Relação das vulnerabilidades identificadas contendo informações detalhadas das vulnerabilidades e orientações e priorização para tratamento.	bloco de ativos (endereços IPs)	4
5	Serviço de Análise de Segurança para descoberta de vulnerabilidades em aplicações	A análise de segurança para identificação de vulnerabilidades em ativos tecnológicos é fundamental para atendimento a Lei, em especial no que diz respeito ao Art. 6, inciso VII que prevê a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados. Essa análise se dará por meio da análise estática de segurança em código fonte de sistemas, aplicações web e aplicativos para dispositivos móveis (SAST) ou pela análise dinâmica de segurança em aplicações web (DAST).	O serviço em questão prevê o emprego de tecnologia para execução de testes e varreduras para descoberta de vulnerabilidades ou fragilidade nos sistemas, aplicações web e aplicativos para dispositivo móvel de modo que seja possível indicar e tratar aquelas que ofereçam maior risco de acessos não autorizados no ambiente ou que possam comprometer a segurança.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Resumo executivo das vulnerabilidades e fragilidades encontradas; - Relação dos sistemas, aplicações web ou aplicativos analisados; - Relação das vulnerabilidades identificadas contendo informações detalhadas das vulnerabilidades e orientações e priorização para tratamento.	bloco de aplicações (código ou URL)	80

6	Serviço de Elaboração de Relatórios e Modelos	Para implementação de estratégias para a privacidade é fundamental que o órgão defina os seus procedimentos voltadas à segurança da informação, de privacidade e cookies, além da elaboração dos relatórios para avaliação dos processos que tratam dados pessoais e seu impacto.	Os serviços contemplam a orientação em Políticas de Privacidade, de Cookies, de Segurança da Informação bem como a elaboração de modelos de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), Análise de Impacto à Privacidade (PIA) e Avaliação de Legítimo Interesse (LIA), todos necessários ao tratamento de dados pessoais.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Política de Privacidade; - Política de Cookies; - Política de Segurança da Informação; - Modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e apoio na aplicação nos processos com alto risco aos titulares; - Modelo de Análise de Impacto à Privacidade (PIA); e - Modelo de Avaliação de Legítimo Interesse (LIA).	serviço	240
7	Serviço de Gestão de Riscos à Privacidade	Uma vez compreendido o cenário de tratamento de dados pessoais é preciso identificar e monitorar os riscos que oferecem risco à organização. Uma vez identificados, será analisado e avaliado para orientar ações de tratamento aos riscos e conformidade.	O serviço em questão é voltado ao levantamento dos riscos à privacidade nos processos que fazem tratamento de dados pessoais, contemplando a definição de métodos e mecanismos para a identificação e avaliação dos riscos e o preenchimento dos relatórios de impacto de dados pessoais (RIPD), resultando na indicação da matriz de riscos bem como o registro e proposição dos controles para tratamento dos riscos. O processo para gestão dos riscos deverá ser implementado na Solução para gestão de estratégia de privacidade.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Mecanismo para ser utilizado durante a etapa de avaliação de segurança dos fornecedores identificados a partir do mapeamento de dados; - Metodologia de gestão de riscos; - Matriz dos riscos à privacidade; - Atividade de análise e avaliação dos riscos à privacidade identificados.	processo	16
8	Serviço de Gestão de Consentimentos e Preferências	O consentimento é uma das principais bases legais apresentadas na LGPD como justificativa legal de tratamento de dados pessoais. Por este motivo a correta gestão deste consentimento se faz tão necessário para aqueles processos que tem esta base legal.	O serviço em questão é voltado a proposição e implementação dos mecanismos para que os titulares possam fornecer e gerir seus consentimentos e preferências, validar operações de tratamento, levantar cookies existentes e disponibilizar scripts para implementação dos banners nos portais.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Lista de portais e formulários que necessitam ser realizadas a gestão de preferências e de consentimentos; - Processo para coleta de consentimento por escrito; - Processo para coleta de consentimento eletrônico; - Processo para revogação de consentimento; - Resultado da avaliação de cookies em cada um dos portais identificados; - Banners para a gestão de preferências em cada um dos portais identificados para a inserção nos mesmos; - Plataforma de gestão de consentimentos customizada de acordo com os processos estabelecidos.	serviço	160
9	Serviço de Gestão de Requisições dos Titulares e Violações de Dados	Um dos pontos fundamentais e que oferecem riscos a uma organização é atender, em tempo hábil, solicitações dos titulares e responder a violações de dados.	O serviço em questão é voltado a definição e implementação desses processos na Solução para gestão de estratégia de privacidade, onde deverão ser elaborados e implementados os procedimentos para o tratamento de solicitações, gestão de violações de dados e gestão de crise.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Procedimento para o tratamento das solicitações dos titulares de dados; - Procedimento de Gestão de Violações de Dados; - Plano de gestão de crise em caso de violações	serviço	64
10	Serviço de Conscientização em Segurança e Privacidade	A implementação de um Programa de Privacidade, além de proporcionar mudanças estruturais e processuais tem por objetivo realizar uma mudança cultural, por meio da conscientização de todos que atuam na empresa, visando o correto tratamento de dados, que reduzirá os riscos de incidentes oriundos de falhas humanas. Identificar fragilidades nas pessoas que atuam na organização e treiná-las é dever da organização para manutenção da segurança.	O serviço em questão visa a realização de eventos de conscientização, remotos e presenciais, relacionados à privacidade e segurança.	Relatório com a consolidação dos resultados obtidos nesta etapa, contendo minimamente: - Programa de Conscientização sobre Privacidade; - Evidências e material utilizado na palestra em evento de conscientização.	evento de conscientização	64
11	Serviço de Simulação de Phishing		O serviço em questão visa a realização de simulações de phishing, utilizando os recursos da Solução para avaliação, conscientização e treinamento em segurança, periodicamente, no intuito de identificar as necessidades para realização de treinamentos para os usuários do Órgão.	Relatório apresentando os resultados alcançados, indicando e justificando os pontos que poderão ser contemplados nas campanhas de treinamento e conscientização.	simulação de phishing	32
12	Serviço de Campanhas de Treinamento		O serviço em questão consiste na avaliação dos resultados alcançados pelas etapas anteriores já concluídas para elaboração e implementação de um plano de treinamento para os diversos perfis de usuários do órgão, utilizando os recursos da Solução para avaliação, conscientização e treinamento em segurança, contemplando a indicação de treinamentos para ciclos de 3 meses.	Relatório contendo o Programa de Treinamento contendo o cronograma e ementa dos treinamentos para cada perfil de usuários contemplados.	campanha	120
13	Serviço de apoio à ISO 27001	Para o cumprimento da política de segurança da informação se faz necessário o estabelecimento de rotinas que orientem os procedimentos ou controles para fins de atendimento às boas práticas no seguimento.	A tarefa consiste em orientar o estabelecimento de rotinas e procedimentos com base nas disciplinas abordadas pela ABNT NBR ISO/IEC 27001 ou frameworks de segurança.	- Manual(is) de segurança e boas práticas	serviço	64

14	Serviço de Análise de conformidade com normas e frameworks de segurança	Realização de análise de conformidade com base em normas e frameworks, tais como CIS Controls, NIST CSF e ABNT NBR ISO/IEC 27001, avaliando os controles indicados por normas e framewrks reconhecidos pelo mercado permitindo identificar, implementar e medir a eficácia dos controles de segurança periodicamente, visando manutenção da conformidade e implementação de novas medidas sempre que oportuno.	O serviço consiste na elaboração de um guia que sirva de modelo para avaliação dos processos que tratam da segurança das informações com base em uma referência normativa ou documento de boas práticas de mercado (framework).	- Relatório de conformidade com os documentos de referência indicados	serviço	352
15	Serviço de operação assistida e repasse do programa ao Encarregado de Proteção de Dados	As organizações devem primordialmente nomear um encarregado responsável por orientar as práticas a serem tomadas para a proteção dos dados pessoais tratados por ela, sendo necessário que o profissional tenha clareza em relação ao seu papel e responsabilidades.	O serviço em questão consiste em atividades para orientar o encarregado bem como elaborar guia orientativo com as atribuições legais do cargo e atividades necessárias a manutenção da privacidade. Para manutenção do programa, ainda como parte desse serviço deverá ser orientar o contratante na elaboração de metodologia(s) para conformidade contínua assim como o apoio, pelo período de 3 meses, para implementação do plano de ação, baseado nesta metodologia.	Relatórios mensal de acompanhamento do Plano de adequação e apoio ao Encarregado, contemplando: - Elaboração do Guia de orientação sobre a definição do Encarregado e papéis no Programa de Governança em Privacidade; - Elaboração de proposta de metodologia de conformidade contínua para governança e gestão da privacidade na organização. - Auxílio na gestão e apoio na implementação do Plano de Adequação, pelo período de 3 meses consecutivos; - Apoio no repasse de conhecimento para operacionalização das operações de tratamento de dados e acompanhamento dos processos executados com suporte das soluções implantadas.	serviço	528
16	Serviço de apoio na operação das soluções e estratégias de privacidade	A Solução de Privacidade e Segurança terá papel fundamental para efetividade de um programa de privacidade e a conformidade com a LGPD, onde para tanto se faz necessário o suporte técnico avançado e a execução por técnicos de atividades de configurações, cargas de dados, administração da solução e o monitoramento de seu funcionamento, em apoio ao Encarregado de Dados.	Os serviços em questão consistem no apoio na operação e administração das Soluções, contemplando entre outros, a avaliação de melhorias em relatórios, indicadores cargas de dados, configuração de alertas e regras, consolidação de informações gerenciais para apoio ao encarregado, registro e repasse das configurações e melhorias implementadas ao longo da prestação dos serviços e outras que se façam necessárias.	Relatório consolidando e evidenciando as atividades executadas no período, contemplando entre outras: - Suporte técnico avançado, configurações, cargas de dados, administração e operação da solução; - monitoramento dos indicadores de privacidade; - Avaliação da eficiência das configurações e indicadores bem como o funcionamento adequado dos processos parametrizados e implementados na solução; - Avaliação de melhorias em relatórios automatizados por meio de novas parametrizações e criação de novos indicadores ou outros elementos que permitam a melhoria do serviço ou processos implementados; - Realizar cargas de dados de informações geradas no decorrer da execução do Contrato; - Configurar alertas e regras que visem auxiliar o Encarregado de Proteção de Dados no âmbito de suas atribuições; - Consolidar e apresentar ao encarregado informações e subsídios para sua atuação, em especial no que tange atividades em atraso ou que ofereçam risco ao órgão; - Apresentar resultados alcançados e indicadores de privacidade ao encarregado.	serviço	176

Rio de Janeiro, 20 de abril de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/04/2023, às 00:29, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Sâmya Massari Lima**, **Diretora**, em 24/04/2023, às 11:50, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Governança e Dados e Informações e

Diretoria de Segurança da Informação

ANEXO III DO TERMO DE REFERÊNCIA

ROTEIRO PARA TESTE DE BANCADA

REQUISITO	ROTEIRO DE TESTES	ATENDE (SIM / NÃO)
1	Apresentar a funcionalidade de geolocalização da informação/fonte de dados classificado e "mapa de calor" dos sistemas com mais dados pessoais e sensíveis	
2	Demonstrar a capacidade de mapeamento automático de dados entre sistemas diferentes, realizando uma “conexão” gráfica entre estes sistemas	
3	Demonstrar a capacidade de mapeamento automático de dados entre sistemas diferentes, realizando uma “conexão” gráfica entre estes sistemas	
4	Demonstrar a classificação de objetos conforme os níveis de sensibilidade e criticidade do conteúdo, e classificação de dados PI (informação pessoal) e PII (informação de identificação pessoal)	
5	Demonstrar a classificação de informações utilizando algoritmos de aprendizado de máquina em dados não-estruturados; suporte para as expressões regulares para encontrar dados pessoais em dados estruturados e não-estruturados; e suporte para OCR para classificar texto nos arquivos JPEG, JPG, BMP, GIF, PNG e PDF e imagens contidas dentro de arquivos Office	
6	Demonstrar a classificação de informações utilizando algoritmos de aprendizado de máquina em dados não-estruturados; suporte para as expressões regulares para encontrar dados pessoais em dados estruturados e não-estruturados; e suporte para OCR para classificar texto nos arquivos JPEG, JPG, BMP, GIF, PNG e PDF e imagens contidas dentro de arquivos Office	

7	Demonstrar que a ferramenta conta com, minimamente, as seguintes expressões regulares nativamente (e com validação/checksum, onde aplica): CPF, CNPJ, PIS, CNH, Título de Eleitor, IPv4, IPv6, IMEI, Email, Endereço MAC e Telefone, permitindo inclusão de novas expressões regulares e suportar a busca de termos próximos ao valor encontrado, para reduzir falsos positivos	
8	Demonstrar a capacidade de adicionar etiquetas nas propriedades dos objetos e colunas, para identificar por exemplo a sua classificação, área responsável, nível de sensibilidade etc. e as etiquetas devem podem ser adicionadas manual ou automaticamente (regras)	
9	Demonstrar a exportação do catálogo em formato CSV e integração por REST API, contando também com capacidade nativa de intercâmbio de metadados com outras ferramentas de catálogo no mercado	
10	Demonstrar a identificação de padrões de documentos através de Machine Learning (por exemplo: fatura, curriculum, contratos etc.), bem como os arquivos duplicados, mesmo que sejam localizados em diferentes sistemas e formatos (DOC, PDF, etc.)	
11	Demonstrar inventario de tabelas de bancos de dados relacionais, exibindo suas colunas e informações básicas, como: chave primaria, tipo de dados definido, tipo inferido, % distintos, % nulos, valores min e max	
12	Demonstrar a capacidade de visualizar de forma prática quantas políticas de conformidade estão sendo infringidas, de acordo com as políticas pré-configuradas da plataforma, prontas para uso, assim como as novas políticas criadas ou políticas existentes customizadas	
13	Demonstrar acionabilidade das políticas infringidas, notificando o responsável do sistema afetado e a capacidade de acionamento automático de ferramentas terceiras por API	
14	Demonstrar a capacidade de instalação em híbrido permitindo que as varreduras ocorrem perto das fontes para minimizar a transferência de dados (performance, ocupação da banda e custos, se aplicam)	
15	Demonstrar a integração com provedores de identidade IDP por protocolo SAML ou LDAP para autenticação de usuários, aplicação do modelo RBAC (com possibilidade de customizações) para definir diferentes perfis de acesso às funcionalidades do sistema, e limitar quais sistemas de dados são visíveis aos quais usuários	
16	Demonstrar a definição de regras personalizadas de qualidade de dados para dimensões como Completude, Acurácia, não Duplicidade, avaliação e acompanhamento das tendencias do desempenho ao longo do tempo	
17	Demonstrar a capacidade de acionamento e alertas dos responsáveis para violações de políticas de qualidade	

18	Demonstrar a definição de políticas de gestão de ciclo de vida de dados para dados estruturados e não-estruturados, que devem ser escolhidos para exclusão	
19	Demonstrar a definição de políticas de retenção legal (dados que não devem ser excluídos apesar que cumprirem prazos de ciclo de sua vida)	
20	Demonstrar a capacidade de executar descobrimento baseados nas políticas de ciclo de vida para encontrar dados obsoletos ou que precisam ser mantidos por questões legais	
21	Demonstrar a capacidade de criação de pelo menos 5 termos e 5 atributos de negócio, com hierarquias de domínios e projetos, e definição de finalidade de uso para justificação de armazenamento dos dados	
22	Demonstrar o workflow de aprovação e revisão, com notificações por e-mail, incluindo as aprovações por parte de responsáveis e certificação final do termo e atributo por supervisor	
23	Demonstrar a capacidade de personalizar os questionários de definição de termo e atributo com os campos adicionais, na ordem preferida, e que sejam obrigatórios ou opcionais, tais como combo, radio, data e lista	
24	Demonstrar a emissão de relatório de acesso aos dados do titular (dossiê), personalizado e com diferentes perfis (de acordo com o relacionamento com o titular, como por exemplo: funcionário, cliente, fornecedor), com registros de consentimento coletados e todas as informações relacionadas ao titular, permitindo a busca de dados pessoais iniciada através do nome ou código único de identificação, como o CPF	
25	Demonstrar a emissão de relatório de acesso aos dados do titular (dossiê) a permitir da requisição e obtenção do dossiê através de API	
26	Demonstrar a capacidade de deleção de dados sobre solicitação do titular ou gestão de fluxo de trabalho com controle de tarefas manuais e mecanismo que garanta que os dados foram de fato excluídos e permaneçam excluídos	
27	Demonstrar a capacidade de solicitações serem feitas pelo próprio titular dos dados através da central de privacidade: (1) acesso aos dados, (2) retificação, (3) remoção dos dados, (4) alteração das preferências de consentimento; com controles de segurança como confirmação positiva de e-mail, telefone e envio de imagens e documentos para comprovação da identidade do solicitante	
28	Demonstrar as notificações automáticas por e-mail informando ao titular solicitante os avanços no atendimento da sua solicitação	

29	Demonstrar a capacidade de integração da ferramenta com fontes terceiras de consentimento do titular, em associação com as respectivas bases legais e propósitos de utilização, e quais dados estão relacionados a elas	
30	Demonstrar a capacidade de criação de questionários personalizados para inventario de dados, com mapeamento dos atores, bases e aplicações envolvidas; e os resultados do descobrimento de dados devem sugerir atualizações do inventario	
31	Demonstrar a capacidade de criação de questionários personalizados para avaliação dos impactos de privacidade, com funcionalidades de colaboração com áreas de negócio e levantamento de riscos automatizado	
32	Demonstrar a capacidade de identificação de dados sensíveis expostos aos usuários externos ou compartilhados publicamente	
33	Demonstrar a integração com ferramentas DLP como MIP, para reforçar a proteção de objetos de dados de acordo com níveis de sensibilidade	
34	Demonstrar a capacidade de orquestração de fluxo de trabalho (workflow) tendo em vista a correção de dados com violações de políticas e problemas de risco, através de: atribuições aos responsáveis pelos dados, automação de ações tomadas, SLAs, colaboração das equipes e trilha de auditoria	
35	Demonstrar a capacidade de investigação do vazamento de dados, com intenção de confirmar se de fato são dados da organização e - caso positivo - identificar a origem do vazamento assim como avaliar o impacto	
36	Demonstrar a capacidade de quantificar risco da organização levando em consideração minimamente a origem de dados (sistema ou base de dados) e classificação (atributos); e este cálculo deve ser atualizado de acordo com os resultados das varreduras (descobrimento automático dos dados)	
37	Demonstrar acesso via Web a console de administração para simulação de phishing e conscientização	
38	Demonstrar a criação de campanha de phishing a partir da construção de e-mail phishing utilizando templates pré-definidos customizáveis	
39	Demonstrar a capacidade de agendar o envio da(s) campanha(s)	
40	Demonstrar/simular o acesso e interação com o conteúdo do e-mail enviado	

41	Demonstrar e interagir com phishing em dispositivo USB	
42	Apresentar os resultados coletados a partir do acesso aos conteúdos na forma de relatório	
43	Apresentar material para conscientização, tais como: cartilhas, papel de paredes, vídeos, etc	
44	Apresentar conteúdo para treinamentos, contemplando vídeos e módulos interativos com conteúdo para identificação de phishing, senhas seguras, LGPD e proteção de dados confidenciais	
45	Demonstrar possibilidade de customização do conteúdo do treinamento	
46	Demonstrar possibilidade de configurar/customizar notificações	
47	Demonstrar relatórios pré-configurados para visualizar o status dos treinamentos bem como a possibilidade do agendamento de envio de relatórios automático para acompanhamento	
48	Demonstrar capacidade para identificar vulnerabilidades de ativos tecnológicos com classificação de riscos cibernéticos para priorização, com acesso autenticado via Web a console de administração	
49	Apresentar relatório de vulnerabilidades de ativos tecnológicos apresentando pontuação para priorização do tratamento das vulnerabilidades com no mínimo os dados do CVSS, idade da vulnerabilidade, número de ativos afetados pela vulnerabilidade e orientações para solução/correção da vulnerabilidade	
50	Comprovar possuir base com no mínimo 50.000 CVE (Common Vulnerabilities and Expossures) para ativos tecnológicos	
51	Demonstrar a capacidade de identificar hosts de ativos tecnológicos no ambiente de forma automática	
52	Demonstrar a capacidade de cadastramento de credenciais para escaneamento em ativos tecnológicos sem exposição das credenciais inseridas	
53	Demonstrar capacidade para identificar vulnerabilidades por meio de análise estática de segurança do código-fonte de aplicações, análise dinâmica de segurança de aplicações web e análise estática de código de aplicações para dispositivos móveis, com acesso autenticado via Web a console de administração	

54	Demonstrar capacidade de realizar varreduras contemplando o Top 10 OWASP, Top 25 VWE, Top 5 PHP, Injeção de SQL, força-bruta e teste completo de penetração contemplando SQL Injection, XSS, inclusão de arquivos, redirecionamento, scan de aplicação no lado servidor	
55	Demonstrar capacidade de comunicar a gravidade de vulnerabilidade determinando urgência e prioridade com pontuação de base, impacto, exploração e temporal	
56	Demonstrar capacidade de realizar análise de código-fonte de aplicações para dispositivos móveis capaz de identificar riscos que fazem parte do Mobile Top 10 do OWASP	
57	Demonstrar capacidade de detectar vulnerabilidades de segurança em aplicações web mapeando estrutura (links e pontos de entrada de dados) utilizando técnicas de análise de código HTML, reconhecimento e preenchimento automático de formulários, seguimento de redirecionamentos, análise e execução de código JavaScript e chamadas XHR	
58	Demonstrar a capacidade de identificar diversos tipos de vulnerabilidade e exposições em aplicações web e aplicações para dispositivos móveis	

REQUISITO	**REQUISITOS A SEREM OBSERVADOS NO TESTE DE BANCADA**	**ATENDE (SIM / NÃO)**
1	Criar, no mínimo, três níveis hierárquicos de contas	
2	Criar usuários, departamentos/órgãos fictícios e grupos de usuários com diferentes permissões e níveis de acesso, os quais deverão ser atribuídos às contas criadas para esta demonstração	
3	Criar catálogos de serviços distintos para, no mínimo, duas unidades administrativas fictícias e seus níveis hierárquicos	
4	Cadastrar, no mínimo, cinco Titulares de Dados externos, com cadastros completos, inclusive com base de CPFs integrada por meio de ferramenta de data discovery ou webservice à base de dados do CONTRATANTE	
5	Gerar relatórios que apresentem os usuários, níveis hierárquicos e departamentos/órgãos que foram criados	

6	Criar um fluxo de operação real, via plataforma 100% web, para receber uma requisição via WEB, desses 5 titulares e fazer o registro completo de uma requisição de serviços na mesma plataforma	
7	Criar um fluxo de operação real, via plataforma 100% web, para receber um pedido de Correção de Dados, de 1 (um) desses Titulares, e, a partir da WEB, fazer o registro completo de uma requisição de serviços na mesma plataforma	
8	Criar um fluxo de operação real, via plataforma 100% web, para receber uma requisição completa de serviço, originada via WEB, que seja parte integrante da mesma plataforma de serviço	
9	Realizar a devolução dessa requisição para o Titular, gerando número de protocolo e resposta automática via e-mail, gerando desta vez ao Titular o Fluxo de Etapas do serviço requisitado, demonstrando possíveis interações via WEB quanto via e-mail	
10	Criar a partir de registro efetuado a abertura de um INCIDENTE fictício, relacionado a problemas de exclusão de arquivo com dados pessoais	
11	Criar o registro de um PROBLEMA a partir do INCIDENTE registrado e resolver a causa-raiz do problema	
12	Criar o registro de uma MUDANÇA para o processo de exclusão proposital de arquivo de dados pessoais, a partir de PROBLEMA registrado	
13	Criar BASE DE CONHECIMENTO, dentro da plataforma web, para a situação INCIDENTE – PROBLEMA – MUDANÇA para o mesmo tipo de situação de modo que o atendente tenha condições de consultar a base de conhecimentos, e então, apresentar a solução para o Encarregado de Dados	
14	Criar um registro de requisição de cliente que demonstre a integração CTI, que desencadeie o fluxo de INCIDENTE, que utilize o processo de resolução, via BASE DE CONHECIMENTO, de modo a evitar o escalonamento para PROBLEMA e MUDANÇA	
15	Apresentar os fluxos de trabalho (workflow) dentro da plataforma web, em interface gráfica, para os processos de INCIDENTE, PROBLEMA e MUDANÇA	
16	Demonstrar a possibilidade de alterações dos fluxos de trabalho (workflow) dentro da própria plataforma 100% web, utilizando-se a interface web para os processos de INCIDENTE, PROBLEMA e MUDANÇA	

17	Criar um item na BASE DE CONHECIMENTO da plataforma web, que contenha elementos de: texto, imagens, áudio e vídeo, e que permita o download de qualquer um desses elementos	
18	Acessar via WEB, e consultar a BASE DE CONHECIMENTO para evidenciar o item criado	
19	Apresentar painel de indicadores da solução para os processos de INCIDENTE, PROBLEMA e MUDANÇA	
20	Apresentar módulo de relatórios da plataforma, e demonstrar todas as possibilidades existentes, com visão de Gerenciamento de Relatórios, Indicadores e Dashboards	
21	Demonstrar que a plataforma web atende todos os requisitos preconizados pela LGPD, relacionados aos gerenciamentos listados a seguir:	
21.1	Gerenciamento de Requisições do Titular e Portal de Serviços	
21.2	Gerenciamento de Incidentes	
21.3	Gerenciamento de Bases Legais, Políticas e Termos	
21.4	Gerenciamento de Terceiros	
21.5	Gerenciamento de Dados não Estruturados	
21.6	Gerenciamento de Dados Estruturados e Inventário de Ativos de Dados Pessoais	
21.7	Gerenciamento de Indicadores da LGPD	
21.8	Gerenciamento de Capacitação da LGPD	
21.9	Gerenciamento de Análise Jurídica	

22	Apresentar integração com repositório de dados estruturados, com no mínimo cinco data sources diferentes (Oracle, MSSQL, MySQL, MariaDB, MongoDB	
23	Apresentar integração com repositório de dados não estruturados, com no mínimo uma integração SMB, CIFS ou DFS e com no mínimo uma integração em nuvem AWS, O365 ou Dropbox	
24	Apresentar formas de criação e busca de dados customizados, demonstrar a criação de um item customizado e a busca em pelo menos uma fonte de dados, o dado customizado poderá ser um CPF em formato diferente	
25	Apresentar a funcionalidade de geolocalização da informação/datasource classificado	

Rio de Janeiro, 20 de abril de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/04/2023, às 00:30, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Sâmya Massari Lima**, **Diretora**, em 24/04/2023, às 11:50, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **49852217** e o código CRC **A9192990**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Governança e Dados e Informações e

Diretoria de Segurança da Informação

ANEXO IV DO TERMO DE REFERÊNCIA

MODELO DE ORDEM DE SERVIÇO / AUTORIZAÇÃO DE COMPRA

1 - IDENTIFICAÇÃO DA ORDEM DE SERVIÇO			
N° do documento:	Data de Emissao:	N° do Contrato:	Data do Contrato:

2 - IDENTIFICAÇÃO DA EMPRESA CONTRATADA		
Nome da Empresa:		
CNPJ:	Inscrição Estadual:	
Endereço:		
Cidade:	UF:	
CEP:	Telefone:	E-mail:

3 - ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	**Descrição do Produto ou**	**Métrica**	**Valor Unitário (R$)**	**Quantidade / Volume**	**Valor Total (R$)**

	Serviço				
...					
TOTAL					

4 – INSTRUÇÕES COMPLEMENTARES

5 – CRONOGRAMA			
tem referente ao Produto/Serviço	**Início Previsto**	**Fim Previsto**	**Prazo Máximo**

6 – CIÊNCIA	
CONTRATANTE	
Gestor do Contrato	**Fiscal Requisitante**
	_____ *<Nome do Responsável pela área requisitante>*

_____ *<Nome do Responsável pela área requisitante>* Matr.: *<nº da matrícula>* Local, *<dd/mm/aaaa>*	Matr.: *<nº da matrícula>* Local, *<dd/mm/aaaa>*
CONTRATADA	
PREPOSTO	
_____ *<Nome do Preposto>* CPF: *<CPF do Preposto>* Local, *<dd/mm/aaaa>*. _____:_____horas	

(*) Trata-se de um modelo de referência, podendo ser aperfeiçoado durante a execução contratual.

Rio de Janeiro, 20 de abril de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/04/2023, às 00:30, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Sâmya Massari Lima**, **Diretora**, em 24/04/2023, às 11:50, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **49852289** e o código CRC **6D6B6272**.

Referência: Processo nº SEI-150016/000013/2022 SEI nº 49852289

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Governança e Dados e Informações e

Diretoria de Segurança da Informação

ANEXO V DO TERMO DE REFERÊNCIA
(a ser incluído como Anexo ao Contrato)

ANEXO xxxx
TERMO DE CONFIDENCIALIDADE E SIGILO

O _____, sediado em _____, CNPJ n.°_____, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____ , CNPJ n. °_____, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE; Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, de dados pessoais de agentes públicos e de cidadãos, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e Decreto Estadual n° 46.475/2018, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo, além da Lei nº 13.709, de 14/08/2018 que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais (Lei Geral de Proteção de Dados Pessoais -LGPD).

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

A vigência deste Termo independe do prazo de vigência do contrato assinado.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, a CONTRATADA assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do CONTRATANTE.

Parágrafo Quarto – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro da _____ , onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

_____, _____ de _____ de 20____

De Acordo.

_____
CONTRATANTE

_____
CONTRATADA

TESTEMUNHAS

Testemunha 1 _____

Testemunha 2 _____

Rio de Janeiro, 20 de abril de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/04/2023, às 00:31, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Sâmya Massari Lima**, **Diretora**, em 24/04/2023, às 11:50, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **49852632** e o código CRC **F4EA4B33**.

Referência: Processo nº SEI-150016/000013/2022 SEI nº 49852632

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Governança e Dados e Informações e

Diretoria de Segurança da Informação

ANEXO VI DO TERMO DE REFERÊNCIA

MODELO DE PLANILHA DE COMPOSIÇÃO DE PREÇO

(Conforme determinado pelo Decreto 46.642/2020, art. 11, XVIII)

Processo SEI Nº_____

Ata de Registro de Preços Nº ____/____

Fornecedor:

OBJETO: **Contratação de empresa para o fornecimento de solução tecnológica de apoio na adequação às obrigações da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.**

LOTE UNICO

Item	ID SIGA	Descrição	Métrica	Quantidade estimada	Valor Unitário (R$)	Valor Total (R$)
1	177603	Subscrição de solução de gestão para adequação e governança de conformidade com a LGPD, incluindo suporte técnico e atualização de software pelo período de 12 meses	unidade			
2	177604	Subscrição de solução de descoberta e mapeamento de dados estruturados e não estruturados, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade			
3	177605*	Subscrição de Solução de Descoberta e Monitoramento de Dados Não Estruturados, com Suporte Técnico e Atualização de Software **(Subscrição de solução para conscientização e treinamento em segurança e privacidade, incluindo suporte técnico e atualização do software pelo período de 12 meses)**	unidade			
4	176272	Subscrição de solução de Gestão de Atendimento a Titulares, Denúncias e Governança de Certificados em conformidade com a LGPD, incluindo suporte técnico e atualização do software pelo período de 12 meses	unidade			
5	177644	Treinamento na Solução de Gestão LGPD	vaga			

6	177646	Serviço de consultoria para apoio na implementação das soluções e adequação à LGPD	UST			
Valor Total a pagamento:						

* para o item 3, ID SIGA/RJ: 177605, considerar a descrição entre parênteses.

- Os preços deverão contemplar todos os custos de acordo com as condições estabelecidas no Termo de Referência.

Rio de Janeiro, 20 de abril de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/04/2023, às 00:31, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Sâmya Massari Lima**, **Diretora**, em 24/04/2023, às 11:50, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **49852700** e o código CRC **96B6A93E**.

Referência: Processo nº SEI-150016/000013/2022 SEI nº 49852700

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone: