SECRETARIA DE ADMINISTRAÇÃO DO ESTADO DO PIAUÍ
Av. Pedro Freitas, 1900, Centro Administrativo, BL1 - Bairro São Pedro, Teresina/PI, CEP 64018-900
Telefone: - http://www.seadprev.pi.gov.br/

MINUTA TERMO DE REFERÊNCIA SEAD

Processo nº 00002.007205/2023-09

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. O presente Termo de Referência tem por objeto o Registro de Preços com vistas a subsidiar a contratação de empresa especializada para a aquisição e implantação de soluções tecnológicas, visando a conformidade e adequação à Lei Nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), do ambiente e operações desta Secretaria de Administração do Piauí - SEAD-PI e outros órgãos da Administração Pública Estadual que possuam dados sensíveis, a ser realizado através de Licitação na modalidade PREGÃO, na forma ELETRÔNICA, conforme especificações, condições e quantidades estimadas, descritas na tabela constante no ANEXO I e II (Estudo Técnico Preliminar e Caderno de especificação técnica da execução do serviço) deste Termo de Referência.

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1. A Justificativa e objetivo da contratação encontram-se pormenorizados no Tópico 2 do Estudo Técnico Preliminar (ID 8775337), ANEXO I deste Termo de Referência.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. A descrição da solução e as definições técnicas do serviço como um todo encontram-se pormenorizados no Tópico 7 do Estudo Técnico Preliminar (ID 8775337), ANEXO I deste Termo de Referência.

3.2. As especificações da execução dos serviços encontram-se descritas no ANEXO II deste Termo de Referência.

3.3. A estimativa da quantidade do objeto deste Termo de Referência deu-se com base na consulta realizada aos órgãos, conforme disposto no tópico 5 do Estudo Técnico Preliminar (ID 8775337), ANEXO I deste Termo de Referência.

3.4. Foi estimado o VALOR TOTAL/GLOBAL de R$ 41.880.999,96 (quarenta e um milhões, oitocentos e oitenta mil novecentos e noventa e nove reais e noventa e seis centavos) , conforme tabelas previstas no ANEXO II deste Termo de Referência.

4. EXIGÊNCIAS DE HABILITAÇÃO

4.1. HABILITAÇÃO JURÍDICA

4.1.1. As exigências de Habilitação jurídica já se encontram previstas na minuta-padrão do Edital da Procuradoria Geral do Estado do Piauí - PGE.

4.2. QUALIFICAÇÃO TÉCNICA

4.3. Qualificação técnico-operacional

4.3.1. Para fins de demonstração da capacidade técnico-operacional, a licitante deverá comprovar aptidão para o desempenho de atividades pertinentes e compatíveis com o objeto deste Termo de Referência, por meio da apresentação de, no mínimo, 01(um) Atestado(s) de Capacidade Técnica, em nome da própria licitante (empresa), fornecido por pessoa jurídica de direito público ou privado, comprovando que a empresa licitante desempenhou ou desempenha as atividades compatíveis o objeto com experiência na implantação de soluções de tecnologia da informação de características e complexidade tecnológica similares ou superior ao objeto contratado.

4.3.2. Deverá explicitar sua experiência no fornecimento, instalação, customização e suporte à solução, incluindo ainda treinamento e capacitação bem como a execução de serviços técnicos especializados para apoio à implantação da solução.

a) Um atestado poderá atender a um ou mais itens.

b) O(s) atestado(s) apresentado(s) deve(m) trazer descrição resumida da solução implantada.

c) O(s) atestado(s) deverá(ão) conter a identificação do emitente, datado, assinado pelo responsável, atestando serviços já executados e concluídos.

d) O(s) atestado(s) poderá(ão) ser alvo de diligência.

4.3.3. Serão aceitos atestados fornecidos em nome da empresa matriz ou da(s) eventual(is) empresa(s) filial(is).

4.3.4. Não será aceita a substituição do Atestado de Capacidade Técnica por cópia de contratos, tendo em vista que a simples existência do contrato não comprova a capacitação técnica da empresa, sendo que o atestado, por ser uma declaração formal do órgão público ou empresa privada, é o único meio de atestar a correta execução dos serviços. Será aceito a cópia do respectivo contrato para a complementação das informações dos atestados apresentados, se necessário.

4.3.5. A licitante deve disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

4.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

4.4.1. Certidão negativa de falência ou de recuperação judicial, expedida pelo distribuidor da sede da pessoa jurídica. Para efeito de constatação da validade de tal certidão, será observado o prazo de validade constante na própria certidão. Caso a licitante esteja em recuperação judicial, será válida, para fins de qualificação econômico-financeira, a emissão de certidão, pela instância judicial competente, que certifique que a interessada está apta econômica e financeiramente a participar de procedimento licitatório, conforme Acórdão TCU nº 1201/2020 – Plenário.

4.4.2. O licitante deverá apresentar os seguintes índices contábeis, extraídos do último balanço patrimonial ou do balanço patrimonial referente ao período de existência da sociedade, atestando a boa situação financeira, conforme art. 7.2 da IN/MARE 05/95, Portaria GAB. SEAD. Nº 88/15, mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), resultantes da aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

4.4.3. As demonstrações contábeis apresentadas poderão ser submetidas à apreciação do Conselho Regional de Contabilidade.

4.4.4. O balanço patrimonial e as demonstrações contábeis, bem como os índices contábeis exigidos, deverão estar assinados por contador ou outro profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade.

4.4.5. A licitante que apresentar índice econômico igual ou inferior a 01 (um) em qualquer dos índices de Liquidez Geral, Solvência Geral e Liquidez Corrente, deverá comprovar que possui patrimônio líquido mínimo não inferior a 10% (dez por cento), do valor total de sua proposta escrita, por meio de Balanço Patrimonial e demonstrações contábeis do último exercício, já exigíveis e apresentados na forma da lei, vedada a sua substituição por balancetes ou balanços provisórios.

4.5. REGULARIDADE FISCAL E TRABALHISTA

4.5.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ).

4.5.2. Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto deste certame.

4.5.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço – FGTS (CRF, fornecido pela Caixa Econômica Federal). Será aceito certificado da matriz em substituição ao da filial ou vice-versa quando, comprovadamente, houver arrecadação centralizada.

4.5.4. Prova de regularidade para com a Justiça do Trabalho emitida pelo TST (Certidão Negativa de Débitos Trabalhistas).

4.5.5. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive

aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

4.5.6. Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei.

5. DA AMOSTRA - PROVA DE CONCEITO - POC

5.1. A Prova de Conceito (PoC) é a oportunidade de se avaliar na prática uma solução ofertada por um determinado fornecedor, buscando, por meio de evidência documentada, subsidiar dados em que se busca estabelecer se este produto ou prestação de serviços atende ou não os requisitos necessários para se obter os resultados necessários demandados pelo interessado. Possibilita também identificar problemas técnicos e logísticos potenciais que podem interferir nestes resultados esperados ou no sucesso da solução.

5.2. A exigência da prova de conceito para os requisitos constantes no Termo de Referência, visa assegurar ao demandante que a aquisição da solução em pauta que atenda aos requisitos funcionais e técnicos solicitados, amenizando os riscos da contratação.

5.3. Ademais, oferece também a oportunidade para que a organização solicite feedbacks (dar resposta a um determinado pedido ou acontecimento) internos ou externos sobre um produto ou serviço em análise, visando mitigar riscos desnecessários que possam impactar ou inviabilizar o uso da ferramenta.

5.4. Outrossim, outros benefícios podem ser sentidos, dentre eles:

a) Eficiência na gestão de recursos;

b) Evidências documentais tangíveis de que a solução atende na prática ou se é viável sua customização ou adaptação;

c) Ganho de confiança por parte dos demandantes, pois passam a visualizar que o projeto pode chegar a resultados satisfatórios;

d) Diminuição dos riscos e aumento da possível satisfação do cliente final, seja ele interno ou externo, com o resultado concreto;

e) Orientação da tomada de decisão, com maior visibilidade e controle.

5.5. Assim, para aceitação da proposta será exigida apresentação de prova de conceito, conforme as condições abaixo:

a) A Prova de Conceito – POC consistirá da apresentação dos requisitos funcionais e técnicos;

b) A primeira licitante classificada deverá comprovar que atende aos requisitos constantes do Termo de Referência que contemplará a aquisição da solução;

c) A solução da licitante, que poderá ser composta por componentes integrados de diferentes fabricantes, deverá atender de forma nativa, 100% dos requisitos funcionais de cada Funcionalidade/serviços na Prova de Conceito.

d) Será desclassificada a licitante que não atender os requisitos exigidos na POC;

e) Os testes para verificação de pleno funcionamento do sistema serão realizados por técnico representante do licitante vencedor com o acompanhamento dos servidores Secretaria de Administração - SEAD, os quais serão responsáveis pela assinatura do Termo de Aceite da solução. Ambos deverão assinar a ata que constará o ocorrido na sessão;

f) A partir da convocação, a licitante terá um prazo de 05 (cinco) dias úteis para dar inicio a prova de conceito nas dependências da Secretaria de Administração - SEAD;

g) A prova de Conceito terá prazo máximo de 15 dias úteis para ser concluída após seu início;

h)Os horários da Prova de Conceito serão das 08:00 às 12:00 e das 13:00 às 17:00;

i) O representante da licitante deverá estar presente durante a apresentação, oportunidade em que esclarecerá as dúvidas ou divergências que possam ser levantadas pela equipe técnica;

j) É direito dos licitantes concorrentes acompanharem os procedimentos relativos à prova de conceito presencialmente; no entanto, não poderão interrompê-la de nenhum modo, sendo-lhes permitido fazer constar pronunciamento em ata;

l) Se o licitante for aprovado na prova de conceito e sua proposta estiver em conformidade com o Edital, ela será aceita e apta a firmar contrato com a Secretaria de Administração - SEAD;

m) Caso o licitante seja reprovado, sua proposta será desclassificada e o segundo licitante colocado terá a oportunidade de apresentar o seu software numa nova prova de conceito;

n) O prazo para a apresentação da segunda colocada será o mesmo da primeira, ou seja, de 5 (cinco) dias úteis, contados a partir da sua convocação.

o) Os itens a serem avaliados na Prova de Conceito estão descritos no Anexo VI.

6. VISTORIA PARA A LICITAÇÃO

6.1. A participação na presente licitação pressupõe o pleno conhecimento de todas as condições para execução do objeto constantes dos documentos técnicos que integram este Termo de Referência, podendo a licitante, caso entenda necessário, optar pela realização de vistoria no local de prestação dos serviços.

6.2. A vistoria será acompanhada por servidor designado para esse fim, em dia e horário previamente agendados, conforme previsão no Edital.

6.3. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

6.4. Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para o ato.

6.5. Eventuais dúvidas de natureza técnica decorrentes da realização da vistoria deverão ser encaminhadas à Comissão de Licitação, através de e-mail do Pregoeiro, indicado no Edital.

7. CRITÉRIOS DE ACEITAÇÃO DA PROPOSTA

7.1. A licitação do objeto consubstanciado neste Termo de Referência é formado por GRUPO ÚNICO contendo 2 (dois) LOTES, conforme tabela constante no ANEXO II deste Termo de Referência.

7.2. Para o julgamento das proposta será adotado o critério de MENOR PREÇO GLOBAL, observada as condições definidas neste Termo de Referência, Edital e Anexos.

7.3. O licitante deverá consignar na proposta comercial o valor UNITÁRIO e o valor TOTAL.

7.4. A proposta comercial terá validade mínima de 90 (noventa) dias, a contar da data da abertura da sessão pública.

7.5. Na elaboração de sua proposta, o licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

7.6. O lance deverá ser ofertado pelo VALOR TOTAL ANUAL do GRUPO.

7.7. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, deverá ser de R$ 50,00 (cinquenta reais).

8. DAS CONDIÇÕES GERAIS DO CONTRATO

8.1. De acordo com o art. 12 do Decreto Estadual nº 11.319/2004, o fato de existirem preços registrados, em nenhum caso, obriga a Administração a firmar qualquer tipo de contratação que deles poderão advir, sendo-lhe facultada a utilização e procura de outros meios, desde que respeitada a legislação respectiva, assegurando-se a todos os possíveis beneficiários do registro preferência e igualdade de condições entre os registrados.

8.2. Conforme disposto no art. 15 do Decreto estadual nº 11.319/2004, todos os fornecedores que tenham seus preços registrados, quando necessário, poderão ser convidados para firmar CONTRATAÇÕES decorrentes do registro de preços, desde que no período de sua vigência e observadas todas as exigências do instrumento convocatório e demais normas pertinentes.

8.3. O(s) contratado(s), após a assinatura do contrato, ficam obrigados ao cumprimento dos prazos e todas as condições estabelecidas previstas neste instrumento, no Edital e no contrato.

8.4. A recusa da execução do objeto ou o não cumprimento de qualquer obrigação prevista ensejará a aplicação das penalidades previstas neste instrumento, no Edital e no contrato.

8.5. Dentro da validade da Ata de Registro de Preços, o fornecedor registrado poderá ser convocado para assinar o contrato, ocasião em que terá o prazo de 05 (cinco) dias úteis para a realização do ato

8.6. O prazo para assinatura do contrato previsto no item 8.5 será prorrogável por igual período, mediante a apresentação de motivo justo e aceito pela parte Contratante, sob pena de decair o direito à contratação, sem prejuízo da aplicação das penalidades cabíveis.

8.7. Da formalização do contrato

8.7.1. Os serviços objeto do presente Termo de Referência serão formalizados mediante Contrato Administrativo, conforme o artigo 57 da Lei nº 8.666/93 e normas editalícias.

8.8. Da vigência do contrato

8.8.1. O prazo de vigência do contrato a ser firmado será de 12 (doze) meses, a contar da data de sua assinatura, prorrogável na forma do art. 57, II, da Lei n° 8.666/93, até o limite de 60 (sessenta) meses, quando comprovada a vantajosidade para a Administração, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

a) Os serviços tenham sido prestados regularmente;

b) Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

c) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

d) Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

e) Seja comprovado que o valor do contrato permanece economicamente vantajoso para a Administração;

f) Haja manifestação expressa da contratada informando o interesse na prorrogação; e

g) Seja comprovado que o contratado mantém as condições iniciais de habilitação.

8.8.2. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

8.8.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo

8.9. Do recebimento dos serviços

8.9.1. As contratações decorrentes deste Registro de Preços devem observar os seguintes prazos para recebimento dos serviços, conforme preceitua o art. 7º, inciso I, do Decreto nº 15.093, de 21 de fevereiro de 2013:

a) provisoriamente, pelo fiscal do contrato, mediante termo circunstanciado, assinado pelas partes em até 05 (cinco) dias da comunicação escrita do contratado;

b) definitivamente, por servidor ou comissão designada pela autoridade competente e presidida pelo fiscal do contrato, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, no prazo máximo de 05 (cinco) dias, sem prejuízo da obrigação de o contratado reparar, corrigir, remover, reconstruir ou substituir , às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, na forma prevista no art. 73, I, “b”, c/cart. 69 da Lei n. 8.666/1993.

8.9.2. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato.

8.9.3. Na hipótese de o termo circunstanciado ou a verificação a que se refere o item 10.10.1 não serem, respectivamente, lavrado ou procedida dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados à Administração nos 15 (quinze) dias anteriores à exaustão dos mesmos, situação na qual será responsabilizado o fiscal ou comissão responsável pela fiscalização.

8.9.4. Prazos de Entrega:

Item	Objeto	Prazo
01	Soluções Tecnológicas (Licenciamento/subscrição)	Até 30 dias corridos após formalização da solicitação por Ordem de Serviço (OS)
02	Serviços Especializados	Sob Demanda e Definido em OS

8.9.5. A CONTRATADA deverá entregar um relatório intitulado Plano de Entrega da Solução, que deverá conter, no que couber, as seguintes etapas:

8.9.5.1. Apresentação da equipe de trabalho;

8.9.5.2. Apresentação do planejamento e cronograma do processo de disponibilização, instalação e configuração das soluções;

8.9.5.3. Visita técnica e solicitação de adequações de infraestrutura do ambiente do CONTRATANTE;

8.9.5.4. Entrega/disponibilização dos componentes de software que compõem a solução;

8.9.5.5. Instalação/disponibilização dos softwares e seus componentes, inclusive configuração;

8.9.5.6. Ajustes necessários.

8.9.6. A CONTRATADA deverá realizar uma visita técnica às dependências do CONTRATANTE e emitir o Plano de Entrega da Solução relacionando as adaptações de ambiente necessárias para a instalação e hospedagem da solução e componentes adicionais que deverá fornecer para integração total da solução ao ambiente do CONTRATANTE. O prazo de entrega do relatório é de 10 (dez) dias corridos, contados a partir da publicação do extrato do Contrato no Diário Oficial.

8.9.7. De posse do Plano de Entrega da Solução, o CONTRATANTE poderá, em até 5 (cinco) dias corridos, solicitar correções visando evitar incongruências entre o ambiente e a solução proposta. As alterações eventualmente propostas pelo CONTRATANTE não interrompem o prazo de entrega da solução.

8.9.8. A CONTRATADA deverá considerar em sua proposta que o CONTRATANTE terá disponível em seu ambiente, infraestrutura suficiente para instalação/disponibilização da Solução.

8.9.9. Após a entrega, o CONTRATANTE, no prazo máximo de 5 (cinco) dias corridos contados a partir da entrega, emitirá o Termo de Recebimento Provisório, assinado pelo fiscal do Contrato.

8.9.10. Os serviços de instalação, disponibilização e configuração deverão ser executados, no que couber, nas dependências do CONTRATANTE, em dias úteis (segunda a sexta feira), no horário das 09:00h às 18:00h.

8.9.11. Caso a CONTRATADA entenda necessário, poderá realizar as atividades de instalação, disponibilização e de configuração em horário diverso do indicado acima, mediante prévia notificação ao fiscal do Contrato.

8.9.12. Todo o processo de instalação, disponibilização e configuração das soluções deverá ser acompanhado e monitorado por profissionais do CONTRATANTE, para esse fim designados.

8.9.13. O prazo máximo para a conclusão da instalação e configuração da solução será de 5 (cinco) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório.

8.9.14. Caso as soluções se encontrem em desconformidade com as exigências desse Termo de Referência, o termo de aceite explicitará as falhas encontradas. A CONTRATADA terá o prazo máximo de 10 (dez) dias corridos para correções e ajustes.

8.9.15. Após a CONTRATADA colocar as soluções em operação, quando aceito pelo CONTRATANTE, será emitido o Termo de Recebimento Definitivo da Solução, assinado pelo fiscal do Contrato, no prazo máximo de 5 (cinco) dias corridos, contados a partir do início da operação da solução.

8.9.16. Critérios de recebimento definitivo: Para emissão do recebimento definitivo os itens entregues serão comparados com as especificações e componentes contidas neste Termo de Referência.

8.9.17. Caso haja inconsistência entre os itens recebidos e os itens solicitados, o prazo de entrega continuará a ser contabilizado até a CONTRATADA sanar a situação.

8.9.18. Os serviços técnicos necessários para a instalação e configuração da solução são de exclusiva responsabilidade da CONTRATADA.

8.9.19. A tabela abaixo resume os prazos para entrega da solução, conforme descrição acima. Os prazos são contabilizados em dias corridos, contados a partir da publicação do extrato do Contrato no Diário Oficial.

Etapa	Descrição	Prazo	Início do Prazo	Responsável
1	Entrega do documento intitulado Plano de Entrega da Solução	5 dias corridos	Publicação do extrato do Contrato	CONTRATADA
2	Entrega/disponibilização da solução de software	30 dias corridos	Publicação do extrato do Contrato	CONTRATADA
3	Emissão do Termo de Recebimento Provisório da Solução	5 dias corridos	Entrega dos componentes de Software da Solução	CONTRATANTE
4	Início dos serviços de instalação, disponibilização e configuração	5 dias corridos	Emissão do Termo de Recebimento Provisório da Solução	CONTRATADA
5	Conclusão dos serviços de instalação, disponibilização e configuração	5 dias corridos	Emissão do Termo de Recebimento Provisório da Solução	CONTRATADA
6	Início da operação da solução	10 dias corridos	Emissão do Termo de Recebimento Provisório da Solução	CONTRATADA
7	Emissão do Termo de Recebimento Definitivo da Solução	5 dias corridos	Início da operação da solução	CONTRATANTE

8.10. Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, quais sejam: qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança.

8.11. Dadas as características dessa aquisição, serão considerados os Níveis Mínimos de Serviço (NMS) que apenas atestarão a adequação da solução entregue aos requisitos definidos e ao cumprimento dos prazos acordados.

8.12. As etapas do projeto devem ser concebidas de forma controlável onde os atrasos dos marcos intermediários não afetam o objetivo comum. Isso também ajuda a evitar sanções associadas aos níveis de serviço.

8.13. Disponibilidade do ambiente das Soluções

8.14. Os serviços da Solução serão considerados integralmente disponíveis quando, em um determinado mês, todos os recursos utilizados na Solução contratada estiverem disponíveis e em pleno funcionamento para a SEAD-PI.

8.15. Serão descartados para efeito de cálculo, todo e qualquer período em que a causa do problema seja identificada como originada do ambiente específico do CONTRATANTE e não da Solução ou serviço contratado, como problemas nos servidores disponibilizados e na rede do Órgão.

8.16. A disponibilidade integral do ambiente será apurada mensalmente, do 1° ao último dia do mês, considerando-se o horário das 0:00:00 às 23:59:00h, de 2ª feira a domingo.

8.17. A disponibilidade integral mínima mensal das soluções, isto é, dos componentes e aplicativos que compõe a solução, deverá ser de 99,7% (noventa e nove vírgula sete por cento), conforme os indicadores a serem considerados a seguir:

DISPONIBILIDADE INTEGRAL DAS SOLUÇÕES – ÍNDICE DE NÍVEL DE SERVIÇO		
INS	Forma de Cálculo	Níveis mínimos (%)
$INS\_Solução$	$INS\_Solução = \frac{(T\ Solução - Ind\_Solução)}{T\_Solução} \times 100$	99,7

8.17.1. Onde:

a) $\boldsymbol{T}\_Solução$: Total de horas do mês considerando a prestação de serviços em regime integral, 24 horas por dia, 7 dias por semana, sem interrupção fora do horário comercial ou em finais de semana e feriados. Será apurado mensalmente, do primeiro ao último dia do mês, considerando-se o horário das 00h00min às 23h59min;

b) $\boldsymbol{Ind}\_Solução$: Quantitativo de horas de indisponibilidade total da Solução, caracterizando um incidente crítico.

8.17.2. Para cálculo das eventuais indisponibilidades, serão considerados os intervalos de tempo decorridos entre a queda e o restabelecimento integral do serviço das Soluções.

8.17.3. As interrupções previamente programadas pela CONTRATADA serão consideradas para o cálculo do período de indisponibilidade e deverão ser comunicadas com antecedência mínima de 2 (dois) dias úteis.

8.18. Tempos Médios de Resposta e Resolução de Problemas

8.19. Tempo Médio de Resposta

Tempo Médio de Resposta					
Indicador		Nível de Problema	Tempo	Meta	Apuração
Tempo Médio de Resposta		Crítico	Em até 30 minutos	99%	Mensal
		Alto	E maté 2 horas		
		Médio	E maté 4 horas		
Baixo	Em até 12 horas				

8.20. Tempo Médio de Resolução

Tempo Médio de Resolução				
Indicador	Nível de Problema	Tempo	Meta	Apuração
Tempo Médio de Resolução	Crítico	Em até 6 horas	99%	Mensal
	Alto	Em até 12 horas		

	Médio	Em até 24 horas		
	Baixo	Em até 96 horas		

8.21. Os níveis de problema seguem premissas consagradas pelo mercado. Fica estabelecido abaixo a descrição de cada um dos níveis de problema:

a) Crítico: Alta criticidade. Indisponibilidade total da solução;

b) Alto: Criticidade média. Indisponibilidade de itens minoritários da solução (Exemplo: incapacidade de fazer acesso ao servidor virtual via VPN, porém com baixo impacto para disponibilidade da solução. Este nível também se aplica para os casos em que há degradação generalizada ou pontual da qualidade do serviço (ex: baixa disponibilidade de banda);

c) Médio: Baixa criticidade. Indisponibilidade de itens minoritários do módulo da solução, tais como incapacidade de acessar painéis gerenciais. Este nível também se aplica para os casos em que há degradação pontual da qualidade do serviço (ex: baixa disponibilidade de banda);

d) Baixo: Requisições gerais e não urgentes, tais como solicitações de novas funcionalidades e/ou dúvidas sobre utilização de recursos.

8.22. Da gestão e da fiscalização do contrato e da Garantia

8.22.1. Nos termos dos Art. 67, § 1º, Lei nº. 8.666, de 1993, a CONTRATANTE designará um representante para representá-lo, acompanhar e fiscalizar a execução do Contrato, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização das falhas ou defeitos observados.

8.22.2. A(s) fiscalização (ões) da(s) contratação (ões) decorrente(s) deste Registro de Preços devem observar o disposto no Decreto nº 15.093, de 21 de fevereiro de 2013, que estabelece procedimentos para o acompanhamento dos contratos firmados por órgãos e entidades estaduais.

8.22.3. Não será exigida garantia de execução contratual.

9. DOS CRITÉRIOS DE SUSTENTABILIDADE

9.1. As contratações decorrentes deste Registro de Preços devem atender aos critérios de sustentabilidade ambiental previstos na especificações do objeto e/ou obrigações da contratada e/ou no Edital como requisito previsto em lei especial.

9.2. O(a) licitante vencedor(a), para a execução dos serviços, objeto do presente Termo de Referência, deverá observar as orientações e normas voltadas para a sustentabilidade ambiental, em especial as contidas no art. 5º e 6º da Instrução Normativa/SLTI/MPOG nº 01, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional, bem como o Decreto nº 7.746/2012, alterado pelo Decreto nº 9.178, de 2017, que regulamenta o art. 3º da Lei nº 8.666/93 para estabelecer critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal direta, autárquica e fundacional e pelas empresas estatais dependentes, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública - CISAP, no que couber, e, ainda:

9.2.1. Adquirir materiais que tenham sido produzidos observando os critérios de sustentabilidade ao meio ambiente, em conformidade com o Decreto nº 7.746, dando preferência para aqueles fabricados com materiais recicláveis;

9.2.2. A licitante vencedora deverá fornecer aos empregados os equipamentos de segurança que se fizerem necessários para a execução de serviços e fiscalizar seu uso, em especial pelo que consta da Norma Regulamentadora nº 6 do MTE;

9.2.3. Para os fins do disposto no art. 2º do Decreto nº 7.746/2012, são considerados critérios e práticas sustentáveis, entre outras:

9.2.3.1. baixo impacto sobre recursos naturais como flora, fauna, ar, solo e água;

9.2.3.2. preferência para materiais, tecnologias e matérias-primas de origem local;

9.2.3.3. maior eficiência na utilização de recursos naturais como água e energia;

9.2.3.4. maior geração de empregos, preferencialmente com mão de obra local;

9.2.3.5. maior vida útil e menor custo de manutenção do bem e da obra;

9.2.3.6. uso de inovações que reduzam a pressão sobre recursos naturais;

9.2.3.7. origem sustentável dos recursos naturais utilizados nos bens, nos serviços e nas obras; e,

9.2.3.8. utilização de produtos florestais madeireiros e não madeireiros originários de manejo florestal sustentável ou de reflorestamento.

10. DA SUBCONTRATAÇÃO

10.1. É permitida a subcontratação parcial do objeto, até o limite de 30% (trinta por cento), na forma do art. 72 da Lei nº 8666/93;

10.2. É vedada a subcontratação completa ou da parcela principal da obrigação;

10.3. A subcontratação depende de autorização prévia da Contratante, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

10.4. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

10.5. A licitante vencedora deverá subcontratar Microempresas e Empresas de Pequeno Porte, nos termos do art. 7º do Decreto nº 8.538, de 2015, nos percentuais mínimo de zero e máximo de 25%, atendidas as disposições dos subitens acima, bem como as seguintes regras:

10.6. A empresa contratada se comprometerá a substituir a subcontratada, no prazo máximo de trinta dias, na hipótese de extinção da subcontratação, mantendo o percentual originalmente subcontratado até a sua execução total, notificando o órgão ou entidade contratante, sob pena de rescisão, sem prejuízo das sanções cabíveis, ou a demonstrar a inviabilidade da substituição, hipótese em que ficará responsável pela execução da parcela originalmente subcontratada;

10.7. A empresa contratada será responsável pela padronização, pela compatibilidade, pelo gerenciamento centralizado e pela qualidade da subcontratação.

10.8. A exigência de subcontratação não será aplicável quando o licitante for:

10.8.1. microempresa ou empresa de pequeno porte;

10.8.2. Os empenhos e pagamentos referentes às parcelas subcontratadas serão destinados diretamente às microempresas e empresas de pequeno porte subcontratadas.

10.9. São vedadas:

10.9.1. a subcontratação das parcelas de maior relevância técnica;

10.9.2. a subcontratação de microempresas e empresas de pequeno porte que estejam participando da licitação;

10.9.3. a subcontratação de microempresas ou empresas de pequeno porte que tenham um ou mais sócios em comum com a empresa contratante.

11. DAS OBRIGAÇÕES DO CONTRATANTE

11.1. As obrigações gerais da Contratante já se encontram previstas na minuta-padrão de contrato da Procuradoria Geral do Estado do Piauí -PGE.

11.2. Obrigações específicas:

11.2.1. Proporcionar todas as facilidades para a CONTRATADA desempenhar o fornecimento do objeto do presente instrumento, permitindo o acesso dos profissionais da CONTRATADA às suas dependências.

11.2.2. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

11.2.3. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

11.2.4. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.

11.2.5. Relacionar-se com a empresa exclusivamente através de preposto por ela indicado.

11.2.6. Prestar as informações necessárias ao desenvolvimento dos trabalhos.

11.2.7. Exigir a qualquer tempo a comprovação das condições da CONTRATADA que ensejaram sua contratação, notadamente no tocante a habilitação na licitação.

11.2.8. Receber, controlar e manter arquivado os documentos entregues pela CONTRATADA.

11.2.9. Não permitir que os empregados da CONTRATADA realizem horas extras, exceto em caso de comprovada necessidade de serviço, formalmente justificada pela autoridade do órgão para o qual o trabalho seja prestado e desde que observado o limite da legislação trabalhista.

11.2.10. Pagar à CONTRATADA o valor resultante da entrega da prestação do serviço, no prazo e condições estabelecidas no Edital e seus anexos.

11.2.11. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela CONTRATADA.

12. DAS OBRIGAÇÕES DA CONTRATADA

12.1. As obrigações gerais da contratada já se encontram previstas na minuta-padrão de contrato da Procuradoria Geral do Estado do Piauí - PGE.

12.2. Obrigações específicas:

12.2.1. Entregar os produtos e serviços conforme especificações deste instrumento e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste instrumento e em sua proposta.

12.2.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os produtos entregues em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

12.2.3. Arcar com prejuízos causados ao CONTRATANTE ou à terceiros, decorrentes de culpa ou dolo durante a execução do Contrato.

12.2.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os Arts. 14 e 17 a 27, do Código de Defesa do Consumidor (Lei 8.078, de 1990), ficando o CONTRATANTE autorizado a descontar da garantia, caso exigida neste instrumento, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos.

12.2.5. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

12.2.6. Apresentar os empregados devidamente uniformizados e/ou identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso.

12.2.7. Apresentar ao CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço.

12.2.8. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade ao CONTRATANTE.

12.2.9. Apresentar, quando solicitado, atestado de antecedentes criminais e distribuição cível de toda a mão de obra oferecida para atuar nas instalações do órgão.

12.2.10. Atender as solicitações do CONTRATANTE quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do Contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste instrumento.

12.2.11. Instruir seus empregados quanto à necessidade de acatar as normas internas do CONTRATANTE.

12.2.12. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo Contrato, devendo a CONTRATADA relatar ao CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.

12.2.13. Relatar tempestivamente ao CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços, ou qualquer situação em que não tenha sido possível a atualização completa de um laboratório, através da elaboração de um Laudo Técnico apresentando detalhadamente o ocorrido e justificando a não conclusão, cabendo ao CONTRATANTE analisar a pertinência ou não da justificada para fins de pagamento total ou parcial da OS em questão, ou suspensão do pagamento para tomada de ações corretivas.

12.2.14. Não permitir a utilização de qualquer trabalho de menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho de menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

12.2.15. Manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

12.2.16. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato.

12.2.17. Repassar ao CONTRATANTE toda a documentação dos produtos gerados na vigência do Contrato, informando e detalhando sua real aplicabilidade, em caso de rescisão ou interrupção contratual.

12.2.18. Durante toda execução contratual deverá ser realizada a transferência de conhecimento para a equipe do CONTRATANTE. Essa transferência de conhecimento deverá conter os elementos suficientes a contemplar a necessidade de transferir à equipe todo o conhecimento e condições para dar continuidade aos serviços em caso de rescisão ou interrupção contratual.

12.2.19. Todos os materiais e produtos relativos e decorrentes da elaboração do trabalho, inclusive códigos-fonte, que sejam produzidos pela CONTRATADA serão de propriedade exclusiva do CONTRATANTE e deverão ser entregues a mesma antes do pagamento da última parcela do Contrato.

12.2.20. Adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa SLTI 01/2010, de 19 de janeiro de 2010, do Ministério do Planejamento e Gestão.

12.2.21. Os profissionais e representantes da CONTRATADA não terão nenhum vínculo empregatício com o CONTRATANTE, correndo por conta exclusiva da CONTRATADA, todas as obrigações decorrentes da legislação trabalhista, previdenciária, infortunística do trabalho, fiscal, comercial e outras correlatas, as quais a CONTRATADA se obriga a saldar na época devida.

13. SANÇÕES ADMINISTRATIVAS

13.1. As sanções já se encontram previstas na minuta-padrão de contrato da Procuradoria Geral do Estado do Piauí - PGE.

14. DA ALTERAÇÃO SUBJETIVA

14.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado.

15. DO PAGAMENTO

15.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

15.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

15.3. Não será autorizado pagamento sem que o fiscal do contrato ateste o recebimento dos serviços descritos na nota fiscal ou fatura apresentada.

15.4. Para execução do pagamento de que trata este item do Termo de Referência, a CONTRATADA deverá fazer constar da Nota Fiscal ou fatura correspondente, emitida sem rasura, em letra bem legível em nome da CONTRATANTE, cujo CNPJ está especificado na qualificação preambular do contrato, informando o número de sua conta corrente, o nome do Banco e a respectiva Agência. 15.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

15.6. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, juntamente com a Nota Fiscal ou fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

15.7. A Nota Fiscal ou fatura correspondente deverá ser entregue, pela CONTRATADA, diretamente ao Fiscal deste Contrato, que somente atestará a execução do objeto e liberará a referida Nota Fiscal para pagamento, quando cumpridas, pela mesma, todas as condições pactuadas.

15.8. Havendo erro na Nota Fiscal ou circunstância que impeçam a liquidação da despesa, aquela será devolvida a CONTRATADA, pelo Fiscal deste Contrato e o pagamento ficará pendente até que se providencie pela CONTRATADA as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal não acarretando qualquer ônus para a Contratante.

15.9. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

I=(TX/100)/365

EM= I x N x VP,

Onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos Moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

15.10. A atualização só será devida em caso de mora imputável exclusivamente ao contratante.

15.11. Para fins de pagamento, a Contratada deverá apresentar os seguintes documentos, conforme Decreto Estadual 15.093/2013, arts. 5º e 6º:

a) Prova de regularidade com o Fundo de Garantia do Tempo de Serviço – FGTS (CRF, fornecido pela Caixa Econômica Federal). Será aceito certificado da matriz em substituição ao da filial ou vice-versa quando, comprovadamente, houver arrecadação centralizada;

b) Prova de regularidade para com a Justiça do Trabalho emitida pelo TST (Certidão Negativa de débitos Trabalhistas);

c) Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

d) Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei.

16. DO REAJUSTE

16.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano. Para fins de reajuste do valor contratual será utilizado o Índice de Preços ao Consumidor Amplo Especial – IPCA-E do período, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

16.2. A atualização dos preços registrados observará os mesmos índices e periodicidade definidos no item anterior para a variação do valor contratual.

17. DA RESCISÃO CONTRATUAL

17.1. O Contrato a ser firmado em decorrência deste Pregão poderá ser rescindido a qualquer tempo, independentemente de notificações ou interpelações judiciais ou extrajudiciais, com base nos motivos previstos nos arts. 77 e 78, na forma do art. 79 da Lei nº 8.666, de 21 de junho de 1993;

17.2. No procedimento que visa à rescisão do contrato, será assegurado o contraditório e a ampla defesa, sendo que, depois de encerrada a instrução inicial, a CONTRATADA terá o prazo de 05 (cinco) dias úteis para se manifestar e produzir provas, sem prejuízo da possibilidade de a CONTRATANTE adotar, motivadamente, providências acauteladoras.

18. RECURSOS ORÇAMENTÁRIOS E FINANCEIROS

18.1. Por se tratar de procedimento licitatório com Sistema de Registro de Preços, os recursos para custeio das despesas decorrentes da contratação que se seguir à licitação de que trata este Termo de Referência correrão à conta das dotações orçamentárias de cada Órgão/Ente do Estado participante do Registro, para os exercícios alcançados pelo prazo de validade da Ata de Registro de Preços, a cargo do CONTRATANTE, cujos programas de trabalho e elementos de despesas específicos constarão da respectiva Nota de Reserva.

19. DAS DISPOSIÇÕES FINAIS

19.1. O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato ou da prestação dos serviços, sem prejuízo das demais sanções cabíveis;

19.2. As normas que disciplinam este procedimento licitatório serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação;

19.3. A participação do proponente neste certame implica em aceitação de todos os termos deste Termo de Referência.

19.4. O foro designado para julgamento de quaisquer questões judiciais resultantes deste Termo de Referência será o do Município de Teresina – Piauí.

20. ANEXOS DO TERMO DE REFERÊNCIA

20.1. ANEXO I - ESTUDO TÉCNICO PRELIMINAR (ID 8775337)

20.2. ANEXO II - CADERNO DE ESPECIFICAÇÃO TÉCNICA DO OBJETO

20.3. ANEXO III - FORMULÁRIO DE AVALIAÇÃO POC

20.4. ANEXO IV - TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES

ANEXO I DO TERMO DE REFERÊNCIA
ESTUDO TÉCNICO PRELIMINAR (ID 8775337)

ANEXO II DO TERMO DE REFERÊNCIA

CADERNO DE ESPECIFICAÇÃO TÉCNICA

1. Das especificações do objeto, condições, quantidades e valores estimados:

GRUPO						
LOTE 1	**Detalhamento dos Itens**	**Unidade de Medida/Aferição**	**QUANT**	**PREÇO REFERENCIAL (METODOLOGIA) MEDIANA**		
	SOLUÇÕES TECNOLÓGICAS (LICENCIAMENTO/SUBSCRIÇÃO)			MEDIANA MENSAL UNITÁRIO	MEDIANA MENSAL	MEDIANA ANUAL
1	Portal Centralizado de Gestão da LGPD	Usuário/Mês	12	R$ 15.000,00	R$ 180.000,00	R$ 2.160.000,00
2	Módulo de Governança de Dados	Bloco de 25 Bases de Dados/Mês	7	R$ 55.000,00	R$ 385.000,00	R$ 4.620.000,00
3	Módulo de Privacidade de Dados	Bloco de 25 Bases de Dados/Mês	3	R$ 55.000,00	R$ 165.000,00	R$ 1.980.000,00
4	Módulo de Segurança de Dados	Bloco de 25 Bases de Dados/Mês	3	R$ 55.000,00	R$ 165.000,00	R$ 1.980.000,00
5	Gestão de Atendimento	Bloco de 25 Bases de Dados/Mês	2	R$ 40.000,00	R$ 80.000,00	R$ 960.000,00
6	Solução de Teste de Penetração	Bloco de 500 Endpoints/Mês	15	R$ 82.000,00	R$ 1.230.000,00	R$ 14.760.000,00
7	Solução de Teste de Penetração	Bloco de 10 Domínios/Mês	15	R$ 3.500,00	R$ 52.500,00	R$ 630.000,00
8	Solução de Anonimização / Criptografia	Unidade	3	R$ 81.000,00	R$ 243.000,00	R$ 2.916.000,00
VALOR TOTAL DO LOTE				**R$ 386.500,00**	**R$ 2.500.500,00**	**R$ 30.006.000,00**
LOTE 2	**DESCRITIVO SERVIÇOS ESPECIALIZADOS**					
1	Serviço de Implantação do item 1	Unidade	3	R$ 16.666,67	R$ 50.000,00	R$ 600.000,00

2	Serviço de Implantação dos itens 2, 3, 4, 5, 6,.7 e 8	Unidade (por módulo, até 4)	18	R$ 13.333,33	R$ 240.000,00	R$ 2.880.000,00
3	Serviço de Hospedagem em Nuvem	Bloco de 25 Bases de Dados/Mês	11	R$ 20.000,00	R$ 220.000,00	R$ 2.640.000,00
4	Serviços de Customização e Desenvolvimento de Integrações	UST sob demanda	5000	R$ 41,67	R$ 208.333,33	R$ 2.499.999,96
5	Serviço de Mapeamento e Análise de Processos de Negócio	UST sob demanda	5000	R$ 41,25	R$ 206.250,00	R$ 2.475.000,00
6	Transferência de Conhecimento	Turma de até 20 Alunos	6	R$ 3.333,33	R$ 20.000,00	R$ 240.000,00
7	Acesso à Plataforma EAD para Segurança da Informação	Aluno/Mês	450	R$ 100,00	R$ 45.000,00	R$ 540.000,00
VALOR TOTAL DO LOTE				R$ 53.516,25	R$ 989.583,33	R$ 11.874.999,96
VALOR TOTAL DO GRUPO				**R$ 440.016,25**	**R$ 3.490.083,33**	**R$ 41.880.999,96**

1.1. O detalhamento do serviço compreende as especificações e condições:

LOTE 1 – SOLUÇÕES TECNOLÓGICAS (LICENCIAMENTO/SUBSCRIÇÃO)

ITEM 1 - PORTAL CENTRALIZADO DE GESTÃO DA LGPD

1. Características Gerais

1.1 A Solução deverá ser fornecida em nuvem, na modalidade SaaS – Software as a Service, para atender os requisitos de privacidade e segurança.

1.2 Todas as funcionalidades da solução que dependam de interação com CONTRATANTE/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.). Não serão aceitas soluções CONTRATANTE/servidor.

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

1.4 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 (clássico e baseado no Chromium), Mozilla Firefox e Google Chrome, independentemente do sistema operacional utilizado (Windows, MAC OS, Linux etc.).

1.5 A solução deverá ser compatível com os navegadores das plataformas de dispositivos móveis: Android e iOS - web adaptativo/responsivo. Alternativamente, poderá ser atendido via aplicativo móvel para as plataformas citadas (app).

1.6 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.

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

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

a. Fundos e banners;

b. Menu e ferramentas de navegação;

c. Campos, formulários e tabelas;

d. Cor do texto, fonte e tamanho;

e. Infográficos, Gráficos e painéis;

f. Alertas e notificações;

g. 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:

- Webservices;
- JDBC;
- LDAP;
- Excel;
- CSV;
- E-mail.

1.9 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.

1.10 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.

1.11 A solução deverá possuir ferramenta de criação de formulários e relatórios, 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.

1.12 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.

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

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

1.15 A solução deve suportar a governança dos dados pessoais de organizações hierárquicas, tais como órgãos de um estado ou empresas de um grupo empresarial, 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:

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

b. 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;

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

d. 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;

e. Por questões de segurança, a solução deverá suportar a instalação dos componentes que necessitam acessar as bases de dados ou dados não estruturados da contratante, tais como data discovery, 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* deverá ser realizada por conexão segura e criptografada.

1.16 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 na modalidade SaaS (*Software as a Service*).

1.17. PADRÕES DA SOLUÇÃO

1.17.1. Todos os aplicativos deverão ser criados em uma única plataforma do CONTRATANTE;

1.17.2. Acesso e interface com o CONTRATANTE da Web - sem a necessidade de aplicativo ou agente local;

1.17.3. Base de dados única;

1.17.4. A solução deve fornecer alta disponibilidade avançada (AHA) em clusters. Os recursos de disponibilidade devem incluir:

1.17.4.1. Possibilidade de redundância total;

1.17.4.2. Tolerância ao erro;

1.17.4.3. Balanceamento de cargas nos servidores;

1.17.4.4. Monitoramento de desempenho;

1.17.4.5. Processo de failover;

1.17.4.6. Backup (Full) e recuperação de desastres;

1.17.4.7. Plano de continuidade de negócios.

1.17.5. A solução deve permitir recursos de personalização para a solução proposta. No mínimo, a solução selecionada deve incluir a capacidade de personalizar:

1.17.5.1. Tema geral (cores, logotipos e imagens);

1.17.5.2. Fundos e banners;

1.17.5.3. Menu e ferramentas de navegação;

1.17.5.4. Campos, formulários e tabelas;

1.17.5.5. Cor do texto, fonte e tamanho;

1.17.5.6. Exibir lista;

1.17.5.7. Site completo;

1.17.5.8. Ul para login, home ou páginas de pesquisa;

1.17.5.9. Infográficos, Gráficos e painéis;

1.17.5.10.Alertas e notificações;

1.17.5.11.Automação de fluxo de trabalho;

1.17.5.12.Integração do sistema.

1.17.6. A solução deve habilitar e suportar a escalabilidade. No mínimo, a solução selecionada deve incluir:

1.17.6.1. Servidores de aplicativos agrupados em cluster;

1.17.6.2. Balanceamento de carga moderno;

1.17.6.3. Teste de escalabilidade;

1.17.6.4. Tempo de resposta do sub-segundo;

1.17.6.5. Nenhuma interação entre nós de cluster;

1.17.6.6. Ambientes multiprocessador / multi-núcleo;

1.17.6.7. Compressão de dados;

1.17.7. A solução deve apresentar controles de segurança e de operações. No mínimo, a solução deve prever:

1.17.7.1. Active Directory / LDAP;

1.17.7.2. Autenticação e início de sessão único;

1.17.7.3. Auditoria e logs do sistema;

1.17.7.4. Segurança das comunicações;

1.17.7.5. Separação de empresas e de domínio;

1.17.7.6. Segurança contextual;

1.17.7.7. Criptografia e integridade de dados;

1.17.7.8. Firewalls e balanceadores de carga;

1.17.7.9. Sistemas de prevenção de intrusão;

1.17.7.10.Segurança e redundância da rede;

1.17.7.11.Controles físicos de segurança;

1.17.7.12.Controles de acesso baseados em funções;

1.17.7.13.Segurança da camada de transporte;

1.17.7.14.Teste de penetração;

1.17.7.15.Vulnerabilidade e gerenciamento de patches;

1.17.7.16.Governança e políticas.

1.17.8. 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:

1.17.8.1. Webservices;

1.17.8.2. JDBC;

1.17.8.3. LDAP;

1.17.8.4. Excel;

1.17.8.5. CSV;

1.17.8.6. E-mail.

1.17.9. A solução deverá 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.

1.17.10. A solução deverá 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.

1.17.11. Além disso, a solução deverá oferecer uma interface rica (Rich Interface) para carregar dados externos usando conjuntos de importação de várias fontes de dados, como HTTPS, FTPS e SCP usando formatos de arquivo, como XML, CSV e Microsoft Excel XLS.

1.17.12. A solução deverá possuir processo de atualização de novas versões. No mínimo, a solução selecionada deve incluir:

1.17.13. Atualizações automáticas de novas versões contendo novas funcionalidades para CONTRATANTEs entregues várias vezes por ano com ótima qualidade e estabilidade;

1.17.14. Novas versões e hotfixes/patchs;

1.17.15. Capacidade de confirmar uma atualização e configurar a notificação de atualização;

1.17.16. Atualizar o histórico e as ferramentas de monitoria de progresso da atualização;

1.17.17. Possuir histórico online de notas de versão para todas as versões anteriores do produto.

1.18. REQUISITOS DE USABILIDADE PARA A EQUIPE DE PRIVACIDADE

1.18.1. A interface de uso e facilidades de manuseio da solução são essenciais para que a experiência dos usuários e sua produtividade sejam as melhores possíveis e para que as pessoas consigam extrair da plataforma os recursos e benefícios esperados para facilitar seu trabalho, executar atividades do dia a dia e gerenciar suas atribuições de forma integrada com outros processos e procedimentos de gestão do CONTRATANTE , Neste sentido, sem a necessidade de programação, a solução deverá:

1.18.1.1. Possuir uma mesma interface (Ex.: estilos de menus, listas e telas de registros, gráficos, dashboards, relacionamento de registros etc.) de navegação e uso em todos os fluxos de trabalho, processos e aplicações que sejam automatizadas dentro da solução.

1.18.1.2. Permitir inserir quantidade ilimitada de anexos em registros de trabalho, fluxos de trabalho e processos automatizados na solução.

1.18.1.3. Opcionalmente, admite-se a utilização de aplicações não nativamente WEB unicamente do lado dos operadores, não sendo admitido do lado do usuário final, para funcionalidades como desenvolvimento de modelos (formulários, relatórios, diagramas de fluxos, calendários, catálogo), exclusivamente para aquelas que dependem de tecnologias que deixaram de ser suportadas por navegadores, devendo-se, ainda assim, serem invocadas pela WEB sem necessidade de instalação prévia de qualquer aplicativo, mantendo-se toda a operação restante possível através de ambiente WEB.

1.18.1.4. A solução deverá possuir interface de acesso totalmente WEB para todas as funcionalidades (administração e uso).

1.18.1.5. A solução deverá possuir interface de acesso e todas suas telas de administração e uso em idioma português padrão Brasil.

1.18.1.6. A solução deverá possuir interface amigável e intuitiva para os usuários e administradores.

1.18.1.7. A solução deverá permitir ser operada em navegadores Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome e Safari.

1.18.1.8. A solução deverá permitir acesso controlado à solução por meio de usuário e senha e com autenticação utilizando serviços de Diretórios LDAP e Microsoft Active Directory-AD.

1.18.1.9. A solução deverá permitir a adequação de menus da interface de atendimento para cada operador, permitindo que o operador organize seus menus com os principais links que utiliza dentro da solução.

1.18.1.10.A solução deverá permitir a criação de menus específicos paras as aplicações e automatizações de fluxos de trabalho e processo do CONTRATANTE, desenvolvidos na solução.

1.18.1.11.A solução deverá permitir o desenvolvimento de formulários, sem a necessidade de programação e diagramação, para a inclusão, exclusão e alteração de campos escolhidos.

1.18.1.12.A solução deverá 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.

1.18.1.13.A solução deve permitir a consulta global por texto livre, pesquisando em textos de eventos, registros e ações.

1.18.1.14.A solução deve permitir a criação de pesquisas e listas de registro sem a necessidade de programação e alteração de código fonte, inclusive por operadores não administradores da solução, a partir da definição dos critérios de pesquisa que devem ser aplicados sobre qualquer campo de um registro de evento.

1.18.1.15.A solução deverá permitir que consultas personalizadas à base de dados podem ser criadas e gravadas para uso posterior pelos times de suporte e gestão, fazendo uso das listas e grids para a apresentação dos resultados.

1.18.1.16.A solução deverá 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.

1.18.1.17.A solução deverá permitir ordenar a lista de registros por qualquer das colunas do grid de visualização, de A a Ze de maior para menor, ou vice-versa.

1.18.1.18.A solução deverá permitir que as listas e grids de registros devem ser separados da janela de registro, permitindo consultar dados de outros registros enquanto realizando um novo cadastro em outra janela, sem consumir mais de uma licença de uso por usuário conectado para este fim,

1.18.1.19.A solução deve permitir ser possível atualizar manualmente as consultas exibidas nas listas e grids (Refresh) sem fechar ou atualizar toda a janela atual do navegador.

1.18.1.20.A solução deve permitir abrir múltiplas listas e grids em janelas diferentes e facilmente alternar entre elas, utilizando apenas uma licença de uso por usuário.

1.18.1.21.O acesso às listas e grids, assim como às informações disponíveis, deve ser controlado por permissões de acesso e perfis de usuário, garantindo que cada usuário somente visualize as informações as quais tem acesso.

1.18.1.22.A solução deverá permitir criar filtros, inclusive com a combinação de mais de um parâmetro de filtro, na lista de registros em qualquer das colunas disponíveis na tela.

1.18.1.23.A solução deverá permitir que usuários realizem pesquisas e filtros avançados.

1.18.1.24.A solução deverá permitir que os usuários exportem para arquivos formato Excel, CSV e XML.

1.18.1.25.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.

1.18.1.26.A solução deverá permitir a alteração de registros, inclusive alterações em lote (vários registros), na própria tela de visualização de registros e grid da solução.

1.18.1.27.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.

1.18.1.28.A solução deverá 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.

1.18.1.29.A solução deverá permitir o relacionamento entre registros de processos, projetos, aplicações e fluxos de trabalho automatizados na solução, sem a necessidade de programação ou alterações do código-fonte.

1.18.1.30.A solução deverá 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.

1.18.1.31.A solução deverá 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:

1.18.1.32.Aprovação por um usuário específico;

1.18.1.33.Aprovação por conjuntos de usuários e regras específicas para sequência de aprovação;

1.18.1.34.Aprovação pelo gerente de um grupo solucionador;

1.18.1.35.Aprovação pelo gerente do solicitante;

1.18.1.36.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);

1.18.1.37.Aprovação por quantidade definida de pessoas em um grupo de solução;

1.18.1.38.Aprovação por vários grupos de solução;

1.18.1.39.Aprovação por grupos de solução juntamente com usuário específico.

1.18.1.40.A solução deverá permitir a configuração, sem alteração de código-fonte, para aprovações que não se enquadram no subitem anterior.

1.18.1.41.A solução deverá permitir atribuir a um usuário ou grupo de usuários específico, o acesso à abertura, modificação e fechamento de registros.

1.18.1.42.A solução deverá permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal.

1.19. INTEGRAÇÃO, INDICADORES E PAINÉIS

1.19.1. A Contratada deverá realizar, para dados estruturados, o data Discovery, integração com portal do titular e gestão jurídica (Data Mapping), seguindo a Política de Gestão e Governança de Dados Corporativo da Contratante, considerando todas as bases de dados utilizados pela Contratante, devendo gerar as seguintes informações.

1.19.2. Dashboard com o resultado do Data Discovery informando quantidade de banco de dados por tecnologia;

1.19.3. Dashboard com o resultado do inventário de servidores analisados (Discos, memória, Ethernet, etc.);

1.19.4. Dashboard com o resultado do Data Discovery por banco de dados, informando quais bancos de dados possuem dados pessoais e/ou sensíveis e a quantidade de colunas que contem cada dado em cada banco de dados.

1.19.5. A Contratada deverá realizar, para dados não estrutuados, o data discovery, data mapping, integração com portal do titular, seguindo a Política de Gestão e Governança de Dados Corporativo da Contratante, considerando todas os repositórios de dados não estruturados utilizados pela Contratante, devendo gerar as seguintes informações.

1.19.6. Dashboard com o resultado do Data Discovery informando quantidade de documentos com dados pessoais e/ou sensíveis;

1.19.7. Permitir criar gráficos e relatórios com o resultado do Data Discovery;

1.19.8. Dashboard com o resultado do Data Discovery por repositório, informando quais diretórios/servidores possuem dados pessoais e/ou sensíveis e a quantidade de dados por tipo (CFP, RG, NOME, etc.).

1.19.9. As integrações deverão ser sugeridas pela CONTRATADA, permitindo que a CONTRATANTE possa estruturar papéis necessários para gestão de informações; definição da estratégia de dados das áreas de negócio; cesta de indicadores que permita:

1.19.10. Medir objetivamente a maturidade das áreas de negócio e TI quanto a disciplinas de gestão de informações;

1.19.11. Medir qualidade das informações;

1.19.12. Eficiência e eficácia dos processos de governança e gestão dedados;

1.19.13. Engajamento das áreas de negócio e TI.

1.19.14. 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. 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.

1.19.15. 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 especializado e de forma intuitiva, criar seus painéis e dashboards de gerenciamento. Para isso, a solução deverá:

1.19.16. 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.

1.19.17. 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.

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

1.19.19. 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.

1.19.20. 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.

1.19.21. 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).

1.19.22. 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.

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

1.19.24. 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.

1.19.25. Permitir a criação de painéis e dashboards com gráficos de gestão a partir de qualquer coluna do banco de dados da solução, sem a necessidade de programação e alteração do código-fonte.

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

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

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

1.20. GERENCIAMENTO DE SERVIÇOS, TAREFAS E INCIDENTES DE NORMAS DE PRIVACIDADE

1.20.1. A solução deve possuir nativamente suporte para os processos de gerenciamento de serviços de TIC a seguir. Para tanto, a solução deverá:

1.20.1.1. Permitir o registro de solicitações de serviços, por meio do portal de serviços ou de tela própria de requisições de serviço.

1.20.1.2. Permitir gerenciar o ciclo de vida de requisições de serviço.

1.20.1.3. Permitir vinculação de várias tarefas para o atendimento de em um mesmo registro de solicitação, inclusive para grupos de atendimento diferentes;

1.20.1.4. Permitir configurar fluxos de trabalho diferentes para cada solicitação, conforme necessidade da CONTRATANTE.

1.20.1.5. Permitir aos atendentes a visualização do fluxo de trabalho, a partir da tela do registro da solicitação.

1.20.1.6. Atender aos requisitos de aprovação de fluxos de trabalho descritos neste documento técnico.

1.20.1.7. Permitir a realização de atendimento da solicitação por fases, permitindo ainda a visualização gráfica das fases de atendimento e situação atual.

1.20.1.8. Permitir a criação de modelos de requisições de serviço permitindo a reutilização para configuração de outras requisições.

1.20.1.9. Deve possuir uma visão baseada em permissões do requisitante dos serviços no catálogo que o usuário tem direito a requisitar.

1.20.1.10.Deve automatizar o roteamento de requisições para a coleta das autorizações apropriadas.

1.20.1.11.Deve permitir que o usuário submeta requisições de serviço, mantenha a visibilidade detalhada do cumprimento da requisição e acompanhe todo o ciclo de vida do cumprimento de sua requisição, sem a necessidade de entrar em contato com a central de serviços para acompanhamento.

1.20.1.12.Deve permitir que indicadores de impacto, prioridade e urgência sejam atribuídos ao registro da Requisição de Serviço.

1.20.1.13.Deve orquestrar os processos de trabalho de requisições complexas através de tarefas sequenciais e paralelas.

1.20.1.14.Deve facilitar a geração de relatórios de requisições de serviço pelo próprio usuário sem a necessidade de intervenção de administradores.

1.20.1.15.Permitir Integração com sistemas de e-mail padrão de mercado, para envio de e-mails (alertas, notificações) de forma automática, ou manual (pelo operador), bem como troca de mensagens entre os profissionais da Tl ou outros usuários da solução.

1.20.1.16.Deve permitir a criação de regras de negócio para requisições específicas ou grupos de requisições, para automatizar processos, tarefas e notificações.

1.20.1.17.Deve suportar a criação de Requisições, a partir de registros de incidentes.

1.21. GERENCIAR FONTES E PROCESSAR DADOS

1.21.1. A solução deverá permitir que na tela principal de gerenciamento, o usuário deverá poder executar as seguintes ações:

1.21.2. Excluir - remove a fonte do processamento; isso será removido dos resultados da pesquisa no devido tempo.

1.21.3. Recolher novamente - enfileira a origem para reprocessamento.

1.21.4. Reindexar - enfileira uma fonte ou item a ser reprocessado, com a verificação de alterações. Se forem encontradas alterações, o item será atualizado e reclassificado.

1.21.5. Reclassificar - enfileira uma origem ou item a ser reclassificado de acordo com as regras de classificação configuradas mais recentes

1.21.6. Pausar - pausa temporariamente o processamento de uma fila

1.21.7. Retomar - retoma o processamento de uma fila pausada

1.21.8. Adicionar ao grupo - permite que uma fonte seja movida para um contêiner lógico (grupo de origem), um grupo existente ou um recém-criado.

1.21.9. A solução deverá permitir, ao clicar no ícone do gráfico, exibir estatísticas específicas da fonte escolhida, de maneira semelhante ao painel principal.

1.21.10. A solução também deverá possibilitar:

1.21.11. Alterar a fonte / grupo selecionando o ícone "engrenagem"

1.21.12. Ver informações detalhadas selecionando o ícone "i"

1.21.13. Navegar até a fonte selecionando o ícone "link"

1.21.14. A solução também deverá possibilitar que ao clicar em uma linha de origem exibirá os dados rastreados diretamente abaixo, com opções ligeiramente reduzidas. Cada linha de origem também mostra estatísticas em cache detalhando o número de registros filho (Documentos) e o tamanho do conteúdo rastreado (Tamanho).

1.21.15. A solução também deverá possibilitar que ao clicar nos níveis possíveis na área de fontes, você pode percorrer toda a estrutura do conteúdo rastreado. Como alternativa, você pode usar ícones para alternar entre a exibição estruturada (pai / filho) e uma exibição plana que mostra todo o conteúdo em uma fonte. Também é possível filtrar a grade por:

1.21.16. Status da página

1.21.17. URL

1.21.18. Tipo (dividido entre tipos e arquivos de contêiner)

1.21.19. A solução deverá permitir verificar a listagem de documentos encontrados através da listagem em tela e através de relatório, contendo a localização de origem.

1.21.20. A solução também deverá possibilitar que cada um dos documentos possua um ícone indicando o tipo de arquivo, além de um link "Informações" que abrirá um pop-up, permitindo que usuário visualize as propriedades, o texto e as classificações do documento.

1.21.21. A solução também deverá possibilitar que cada documento também possua um status associado, mostrado em formato numérico. Ao clicar no número, será exibida uma representação textual do status.

1.21.22. A solução deve permitir a gravação de informações de classificações no sistema, com o campo de metadados gerenciados do SharePoint. Deverá conter um indicador se a gravação foi bem-sucedida ou se a gravação falhar, com descrição em texto identificando a falha.

1.21.23. A solução também deverá possibilitar que ao adicionar / gerenciar configurações de origem, as configurações mais usadas são exibidas por padrão. Possibilitar configurações adicionais dependendo da fonte.

1.22. CAPACIDADES DE GERAÇÃO DE RELATÓRIOS

1.22.1. A solução deve possuir uma área de gestão da ferramenta possibilitando a emissão de relatórios. O painel principal deverá possuir três gráficos de alto nivel, destacando o estado atual do processamento:

1.22.1.1. Progresso do documento - Uma exibição gráfica da exibição principal de estatísticas, assim que o processamento estiver concluído, os documentos serão alocados para totalmente processado ou erros;

1.22.1.2. Tamanho do índice - mostra a porcentagem de cada tipo de fonte sendo processada: arquivos, SharePoint, SQL e fontes da Web;

1.22.1.3. Cobertura de classificação - mostra a porcentagem de conteúdo classificado, discriminada por tipo, e a porcentagem de conteúdo que não recebeu nenhuma classificação automática.

1.22.2. A solução deve possibilitar filtrar e refinar a exibição, procurar as áreas que contêm a maior quantidade de documentos marcados com um termo específico ou revisar apenas conteúdo específico.

1.23. REQUISITOS DE SEGURANÇA

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

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

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

1.23.4. A solução deve prover mecanismo de segundo fator de autenticação;

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

1.23.6. 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;

1.23.7. A solução deve ter a funcionalidade de criação de perfis de Controlador, Jurídico, 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.

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

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

1.23.10. 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;

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

1.23.12. 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;

1.23.13. A plataforma da solução deve possuir recursos para garantir a segurança das informações em trânsito e em repouso; 1.23.14. Quanto aos requisitos de segurança da aplicação, a solução deve atender, no mínimo, aos requisitos de segurança do framework OWASP;

1.23.15. Pré-requisitos para o ambiente SaaS:

1.23.16. O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27017:2015;

1.23.17. O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27001:2013;

1.23.18. O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27018:2019;

1.23.19. O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27701:2019;

1.23.20. O fabricante deve possuir em seu site evidências de que possui o relatório SSAE 18 SOC 1 e SOC 2;

1.23.21. A solução deve fornecer alta disponibilidade avançada (AHA) em clusters;

1.23.22. O fabricante deve atender ao Padrão BSI Cloud Computing Compliance Controls Catalog (C5);

1.23.23. O fabricante deve possuir em seu site evidências de que possui a Certificação Cyber Essentials Plus;

1.23.24. O fabricante deve possuir reconhecimento de Privacidade da APEC para Processadores (PRP)

1.23.25. O fabricante deve possuir ASD IRAP avaliado para serviços em nuvem OFICIAIS E PROTEGIDOS

1.23.26. O fabricante deve possuir deve ter Relatório SOC 2 + HITRUST

1.23.27. O fabricante deve possuir deve ter Certificação Cyber Essentials Plus

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

1.23.29. 99,8% de disponibilidade ou mais;

1.23.30. Centros de dados (Datacenters) espelhados localizados em território nacional;

1.23.31. Redundância total;

1.23.32. Tolerância ao erro;

1.23.33. Balanceamento de cargas nos servidores;

1.23.34. Monitoramento de desempenho;

1.23.35. Processo de failover – RTO de 2 horas e RPO de 1 hora, no máximo;

1.23.36. Backup (Full) e recuperação de desastres;

1.23.37. Plano de Continuidade de Negócios.

1.24. INTERFACE MOBILE PARA A EQUIPE DE PRIVACIDADE

1.24.1. A velocidade exigida pelo negócio, tanto em operações de Privacidade, 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 fundamental que a solução disponibilize meios práticos e modernos de interação das pessoas com suas funcionalidades por meio de dispositivos móveis. Com isso, sema necessidade de programação, a solução deverá:

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

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

1.24.1.3. Poder tomar decisões e realizar ações que possam afetar o fluxo de um workflow;

1.24.1.4. Poder visualizar e adicionar anexos;

1.24.1.5. Poder acessar menus configurados e personalizados na solução WEB;

1.24.1.6. Possuir chat e mensagens instantâneas entre usuários da solução;

1.24.1.7. Possuir notificações do tipo push.

1.25. REQUISITOS DO MÓDULO DE ATENDIMENTO AOS DIREITOS DOS TITULARES

1.25.1. A solução deve ter capacidade para receber, processar e registrar uma solicitação de acesso dos titulares de dados;

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

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

1.25.4. 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;

1.25.5. A solução deve fornecer recursos de atribuição automática e retribuição conforme necessário para cada ticket de solicitação de titulares;

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

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

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

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

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

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

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

1.25.13. 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 Controlador sempre que um SLA não for cumprido;

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

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

1.25.16. A solução deve possuir recursos de geração de relatórios personalizados;

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

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

1.25.19. 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.

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

1.26. GERENCIAMENTO DE NÍVEL DE SERVIÇO PARA AS SOLICITAÇÕES E ACOMPANHAMENTOS DOS DIREITOS DOS TITULARES

1.26.1. 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:

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

1.26.1.2. 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

1.26.1.3. 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.

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

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

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

1.26.1.7. Permitir definição de múltiplos SLA.

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

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

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

1.26.1.11. Permitir gerenciar o ciclo de vida de SLA.

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

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

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

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

1.26.1.16.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).

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

1.26.1.18.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

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

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

1.26.1.21.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.

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

1.27. BASE DE CONHECIMENTO SOBRE NORMAS DE PRIVACIDADE, POLÍTICAS, TERMOS E NORMAS

1.27.1. O gerenciamento do conhecimento de uma organização é fundamental não só para sua agilidade na entrega de serviço, mas também para a continuidade de seus serviços. Com isso, a solução deverá:

1.27.1.1. Possuir uma base de dados para armazenamento de artigos de conhecimento da organização.

1.27.1.2. Permitir configurar e gerenciar o ciclo de vida de registros de artigos de conhecimento.

1.27.1.3. Possuir recursos de pesquisa de soluções aos usuários enquanto registram as solicitações;

1.27.1.4. Possuir recurso para busca indexada, apresentando soluções para os atendentes;

1.27.1.5. Permitir classificar e atribuir categorias e pesos para o conhecimento;

1.27.1.6. Permitir a pesquisa de artigos de conhecimento nas telas de atendimento de registros dos processos de gerenciamento de incidente, mudança, problema, requisições.

1.27.1.7. 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.

1.27.1.8. Permitir gerenciar documentos de conhecimento estabelecendo prazos de validade e de revisão.

1.27.1.9. Permitir o gerenciamento de acesso de usuários aos artigos de conhecimento.

1.27.1.10.Permitir inserir ou anexar imagens, vídeos e textos em documentos de conhecimento.

1.27.1.11.Permitir a criação, adição, manutenção e remoção de artigos de conhecimento em uma estrutura definida e hierárquica de conhecimento.

1.27.1.12.Permitir pesquisar através de palavras-chave ou frases inteiras.

1.27.1.13.Deve controlar o processo de aprovação de um documento, antes do mesmo ser publicado na base de conhecimento.

1.27.1.14.Deve 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.

1.27.1.15.Deve possuir uma interface fácil e iterativa para a consulta a base de conhecimento, tanto para o analista quanto para o usuário final.

1.27.1.16.Possuir lista de perguntas frequentes (FAQS) para cadastrar informações sobre problemas conhecidos, erros comuns, rotinas e procedimentos, permitindo a categorização das informações inseridas.

1.27.1.17.Deve possibilitar rastrear, automaticamente, quantas vezes um artigo ou informação de conhecimento foi utilizado.

1.27.1.18.Deve apresentar 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 associação de documentos e artigos de conhecimento a eventos de Incidentes, Problemas e Mudanças.

1.28. BANCO DE DADOS DE GERENCIAMENTO DE CONFIGURAÇÃO - BDGC.

1.28.1. Quanto ao inventário de ativos de tecnologia, gerenciamento de ativos e itens de configuração, mapeamento de modelos de configuração de serviços e definição de linhas de base de configuração, a solução deverá:

1.28.1.1. Prover a descoberta de toda a infraestrutura, Itens de Configuração e seus respectivos relacionamentos de forma automática sem agentes instalados em ambiente on-premises ou em nuvem, para a população do BDGC.

1.28.1.2. Prover a descoberta dos serviços de negócio "top down" e criar um mapa abrangendo todos os dispositivos, aplicações e perfis de configuração referente a estes serviços de negócio.

1.28.1.3. Possuir uma base única de gerenciamento de ativos e itens de configuração podendo gerenciar tais itens independentemente da metodologia ou processo e que permita sua população de forma automatizada e manual.

1.28.1.4. Permitir inventariar e mapear serviços de negócio hospedados em nuvem privada, pública, híbrida ou em recursos locais.

1.28.1.5. Permitir a configuração de informações de cada tipo de ativo, permitindo adicionar e remover campos de informações de gestão do ativo.

1.28.1.6. Permitir o acesso seguro e controlado à base de dados do gerenciamento da configuração.

1.28.1.7. Deve implementar e seguir corretamente o fluxo de Gerenciamento de Configuração e Ativos de Serviço conforme prescrito na biblioteca ITIL V3 e deve permitir no mínimo:

1.28.1.8. Manter atualizadas características da configuração de ativos;

1.28.1.9. Manter atualizadas características da configuração de componentes de ativos;

1.28.1.10.Manter atualizados os relacionamentos entre ativos com possibilidade de representação gráfica destes relacionamentos;

1.28.1.11.A representação gráfica do relacionamento entre ativos deve permitir o drilldown de informações, para obter detalhes do ativo, seus relacionamentos, seus usuários, ou seus componentes.

1.28.1.12.Permitir a criação manual de itens de configuração a partir de modelos pré-definidos (templates), para agilizar o preenchimento de informações e criação de relacionamentos entre ativos.

1.28.1.13.Permitir a criação livre de itens de configuração, para o registro e controle de itens que não se aplicam sob um padrão.

1.28.1.14.Permitir a criação manual de itens de configuração para aqueles tipos de ativos que não sejam eletronicamente inventariáveis.

1.28.1.15.Permitir o complemento de informações de um ativo, que não puderam ser eletronicamente inventariadas ou que não estavam disponíveis.

1.28.1.16.Permitir também o cadastro de itens não técnicos, como mobiliário, equipamentos que não pertençam à TI, dentre outros, sem prejuízo à capacidade de relacioná-los com outros itens, técnicos ou não, para a representação gráfica dos relacionamentos

1.28.1.17.Permitir o gerenciamento de todo o ciclo de vida do ativo, de acordo com as definições da biblioteca ITIL V3 ou conforme necessidades do CONTRATANTE.

1.28.1.18.Deve prover uma hierarquia de produtos que possua, pelo menos, uma classe, uma categoria, um tipo e seus itens. Exemplo: Software > Aplicações de Escritório > MS Office > Licença XYZ do MS Office 2010. Ou conforme necessidades de personalização do CONTRATANTE

1.28.1.19.Deve permitir a definição de atributos personalizáveis para itens de configuração, tais como, mas não limitado, a número de série, patrimônio, versão, localização, carga e taxa de depreciação.

1.28.1.20.Deve suportar a federação e reconciliação de dados com fontes de dados externas, para permitir manter as informações de ativos em bases de dados distintas do BDGC.

1.28.1.21.Oferecer um conjunto mínimo de relatórios gerenciais sobre itens de configuração, ativos e informações financeiras, para facilitar os processos de auditoria do Gerenciamento da Configuração e permitir a criação de relatórios e dashboards conforme as necessidades do CONTRATANTE.

1.28.1.22.Deve permitir a rápida identificação, recuperação e análise de todas as Requisições de Mudança associadas a um mesmo item de configuração.

1.28.1.23.Deve permitir a rápida identificação, recuperação e análise de todas os registros de incidentes e problemas associados um item de configuração.

1.28.1.24.Prover o inventário das informações de hardware de estações de trabalho e servidores tais como: processador(es), memória, placa mãe, interface(s) de rede, protocolos de rede, System BIOS, System Slots, portas de 1/0, Devices, Discos (físicos e lógicos), file systems, recursos do sistema operacional, settings de região, controladoras (IDE, SCSI, USB) e outros, além de permitir a coleta e inserção de dados de inventário a partir do uso de arquivos externos.

1.28.1.25.Possibilitar a coleta, em plataforma Windows e Linux (servidores de rede), dos serviços existentes e as informações associadas a estes (Status, descrição etc.).

1.28.1.26.Deve ter um BDGC centralizado, para acesso a partir de qualquer processo nativo da solução ou fluxo de trabalho que tenha sido automatizado na solução.

1.29. REQUISITOS DO MÓDULO DE GESTÃO DE CONSENTIMENTOS.

1.29.1. A Solução deve possuir um módulo para gestão de consentimento para o tratamento de dados pessoais;

1.29.2. A gestão do consentimento deve ser integrada aos demais módulos 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.

1.29.3. 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.

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

1.29.5. 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);

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

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

1.29.8. 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;

1.29.9. A Solução deve permitir que aplicações da contratante possam consultar o prazo de validade do consentimento, conforme técnicas especificadas no item 7.36.1;

1.29.10. 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;

1.29.11. 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 processo de negócio possuem consentimento para uso de dados pessoais, quantos titulares concederam o consentimento, e quantos titulares revogaram o consentimento;

1.29.12. A Solução deve fornecer um painel de controle central e recursos de relatórios que permitam ao Controlador avaliar o status, histórico, estatísticas 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;

1.29.13. 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;

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

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

1.30. REQUISITOS DO MÓDULO DE GESTÃO DE TERCEIROS

1.30.1. A solução deve permitir a avaliação de fornecedores e de terceiros;

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

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

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

1.30.5. 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;

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

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

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

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

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

1.30.11. 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;

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

1.31. REQUISITOS DO MÓDULO DE GESTÃO DE RISCOS.

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

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

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

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

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

1.31.6. 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;

1.31.7. 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;

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

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

1.31.10. A solução deve suportar pontuações de risco customizáveis;

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

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

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

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

1.32. REQUISITOS DO MÓDULO DE GESTÃO DE INCIDENTES

1.32.1. 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;

1.32.2. 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;

1.32.3. 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;

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

1.32.5. 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;

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

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

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

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

1.32.10. 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);

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

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

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

1.32.14. 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.

1.33. REQUISITOS DO MÓDULO DE GESTÃO DE AVISOS DE PRIVACIDADE E GESTÃO DE COOKIES.

1.33.1. 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;

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

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

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

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

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

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

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

1.33.9. 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;

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

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

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

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

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

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

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

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

1.33.18. 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;

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

1.33.20. Todos os cookies e instâncias de outras tecnologias de dados do site encontrados;

1.33.21. identificar as tecnologias de captura de dados de cookies/site não declaradas nas políticas de cookies.

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

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

1.33.24. Deve suportar diferentes idiomas para os banners de cookies;

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

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

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

1.33.28. Deve permitir o agendamento periódicos de auditorias;

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

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

1.34. REQUISITO DO MÓDULO DE PRIVACY BY DESIGN/DEFAULT.

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

1.34.2. Proativo, e não reativo; preventivo, e não corretivo

1.34.3. Privacidade como padrão (Privacy by Default)

1.34.4. Privacidade incorporada ao design

1.34.5. Funcionalidade total (soma positiva, não soma-zero)

1.34.6. Segurança de ponta a ponta

1.34.7. Visibilidade e transparência

1.34.8. Respeito pela privacidade do usuário

1.35. COMUNICAÇÃO INTEGRADA PARA O DPO, EQUIPE DE PRIVACIDADE, JURÍDICO, TI E TITULARES DE DADOS.

1.35.1. 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 de Privacidade . Para tanto, sem a necessidade de programação, a plataforma deverá:

1.35.2. Permitir a comunicação em tempo real entre CONTRATANTEs, usuários e atendentes dos serviços por meio de chat integrado à plataforma

1.35.3. permitir que anotações de trabalho sejam registradas nos registros da solução, dando a opção aos operadores atendentes de publicar e deixar visível ou não para usuários solicitantes.

1.35.4. 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:

1.35.5. poder inserir notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados na solução.

1.35.6. poder enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementado na solução.

1.35.7. poder enviar notificações baseadas em condições e eventos da solução incrementados ou alternados

ITEM 2– MÓDULO DE GOVERNANÇA DE DADOS:

2. Características Gerais

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

2.2 Permitir definição de políticas para retenção legal (ex. dados dos ex-funcionários, ações na justiça) ou outros motivos de retenção (ex. pendência financeira).

2.3 Permitir criação de políticas em critério de tempo (filtro de data)

2.4 Permitir criação de políticas de retenção de dados em critério de metadados (ex. data de criação, modificação, formato etc.).

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

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

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

2.8 Permitir exportação e importação de políticas.

2.9 Permitir a criação de políticas em critério de correlação, por exemplo, específico grupo de personas (funcionários, clientes etc.) ou produtos (por exemplo, apólices).

2.10 Permitir a geração de consultas para fontes estruturadas para identificação de dados para remoção, considerando retenção legal.

2.11 Permitir a definição de regras personalizadas de qualidade de dados nas categorias como completude, consistência, acurácia etc.

2.12 Permitir gestão de regras de qualidade de dados em linguagem natural

2.13 Permitir tomar ações para os dados que não cumprem esperados níveis de qualidade através de integração com aplicação de Remediação.

2.14 Permitir notificar aos proprietários dos dados sobre eventos de avaliação.

2.15 Permitir avaliação de dados com o "*Machine Learning*" para obter orientação sobre valores discrepantes e sugestões de problemas de qualidade.

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

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

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

2.19 Permitir gerenciamento proativo de qualidade de dados.

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

2.21 Permitir acompanhamento das tendencias da qualidade na linha de tempo.

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

2.23 Integrar para o catálogo as pontuações de níveis de qualidade de dados.

2.24 Permitir comparar diferentes objetos de dados para comparar os metadados coletados.

2.25 Oferecer um gerenciador de tarefas para que os *Data Stewards* possam priorizar e organizar seu o trabalho.

2.26 Permitir colaboração entre os *Data Stewards*, os proprietários por parte de negócio e proprietários técnicos dos ativos.

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

2.28 Possuir técnica de "*Machine Learning*" para recomendar invés de ter que selecionar manualmente os glossários de negócios.

2.29 Permitir associação automática dos termos lógicos do glossário (termos de negócio) com os ativos físicos, em escala.

2.30 Permitir pesquisa de glossário de negócio para que os usuários possam encontrar os termos e/ou os atributos de interesse.

2.31 Permitir criação de hierarquias de domínios, atributos e termos para melhor organização da estrutura e compreensão.

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

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

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

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

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

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

2.38 Permitir a realizar uma análise de linhagem de negócio, no nível do termo e atributos de negócio associados.

2.39 Permitir a inclusão de novos campos nas definições de termos e atributos de negócio, como *radio-box*, *drop-box*, *check-box*, datas etc.

2.40 Permitir a execução da descoberta de dados (Data Discovery) para fontes de dados estruturados para no mínimo as seguintes bases de dados:

- ADABAS;
- Oracle;
- MSSQL;
- MySQL;
- MongoDB.

ITEM 3 – MÓDULO DE PRIVACIDADE DE DADOS

3. Características Gerais

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

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

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

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

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

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

3.7 Permitir deleção de dados sobre solicitação do titular ou gestão de fluxo de trabalho com controle de tarefas manuais.

3.8 Permitir emissão do dossiê em formato PDF ou CSV.

3.9 Fazer a busca de dados do titular automaticamente (sem intervenção) e sob demanda, buscando sempre os dados mais atuais nas fontes de dados.

3.10 Permitir solicitações em lotes, por mais que um titular numa solicitação.

3.11 Permitir diferentes perfis de dossiê, de acordo com o relacionamento com o titular, exemplos: funcionário, ex-funcionário, contratante, fornecedor etc.

3.12 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.

3.13 Prover um portal de autoatendimento para que o próprio titular possa realizar suas solicitações.

3.14 Permitir, no mínimo, solicitações de acesso, retificação e remoção dos dados, bem como alteração das preferências de consentimento.

3.15 Possuir integração com protocolo OAUTH para autenticação dos solicitantes.

3.16 Permitir controles de segurança como confirmação positiva de e-mail e telefone para validação dos dados.

3.17 Permitir customização do questionário de solicitação.

3.18 Permitir envio de imagens e documentos para comprovação da identidade do solicitante.

3.19 Permitir a configuração de fluxos de trabalho, possibilitando inclusive a entrega completamente automatizada do relatório final para o titular.

3.20 Fornecer *dashboard* para que o gestor de privacidade possa ter uma visão agrupada das requisições, minimamente: data, tipo da solicitação, e prazo/em atraso.

3.21 Fornecer ao titular uma interface com os dados originais e permiti-lo alterar estes dados.

3.22 Permitir ao gestor a revisão das informações antes de serem enviadas ao solicitante.

3.23 Possuir auditoria das solicitações, dos revisores e dos aprovadores.

3.24 Ser capaz de ler diversas fontes de consentimento para identificar quais consentimentos foram dados por cada titular.

3.25 Permitir documentação dos termos de privacidade disponíveis, com sua localização (URL), versão e tempo de validade, relacionando-os às bases legais.

3.26 Permitir emissão de um relatório das bases legais, e quais dados estão relacionados a elas.

3.27 Permitir emissão de um relatório de propósitos de utilização, e quais dados estão relacionados a eles.

3.28 Permitir registro de consentimento do titular.

3.29 Permitir gestão de consentimento do titular.

3.30 Permitir validação do consentimento e violações.

3.31 Permitir integração de base externa com registros de consentimento.

3.32 Permitir documentação dos termos legais de consentimento.

3.33 Permitir documentação do propósito de armazenamento dos dados.

3.34 Permitir documentação da base legal para armazenamento de dados.

3.35 Permitir múltiplos canais de consentimento (contratante, fornecedores, funcionário etc.).

3.36 Permitir customização de acordos, baseados em regulamentações ou políticas internas.

3.37 Oferecer ao titular centro de gestão de preferências.

3.38 Correlacionar automaticamente os consentimentos e preferências.

3.39 Identificar todos os cookies e outras tecnologias de coleta de dados estão sendo utilizadas nos *sites*.

3.40 Incluir a auditoria de páginas *web* onde a autenticação do usuário é necessária.

3.41 Fornecer uma descrição de uso para cada um dos *cookies* de terceiros e outras tecnologias de coleta de dados do site identificadas na varredura.

3.42 Possuir a capacidade de gerar relatórios: todos os *cookies* e instâncias de outras tecnologias de dados do *site* encontrados.

3.43 Possuir a capacidade de gerar relatórios: identificar as tecnologias de captura de dados de *cookies/site* não declaradas nas políticas de *cookies*.

3.44 Possuir a capacidade de produzir uma política de *cookies* atualizada para cada domínio com base nos resultados da auditoria de *cookies*.

3.45 Possuir a capacidade de criar um *banner* de *cookies* personalizado para cada *site* verificado.

3.46 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.

3.47 Registrar o consentimento de *cookies* dos visitantes dos *sites*.

3.48 Possuir a capacidade de adicionar uma descrição de *cookies* novos/desconhecidos antes da política de *cookies* ser publicada.

3.49 Permitir que realização das auditorias automatizadas não degrade ou prejudica o desempenho em tempo real dos *sites* auditados.

3.50 Permitir auditorias automatizadas realizadas pelo menos a cada trimestre.

3.51 Possuir a capacidade de reter relatórios de cookies para cada página verificada e rastrear as mudanças.

3.52 Possuir a capacidade de bloquear automaticamente os *cookies* das categorias as quais o visitante não deu consentimento.

3.53 Permitir mapeamento de processos de negócios, atores, bases de dados e aplicações envolvidas.

3.54 Permitir gestão e visibilidade de atividades de processamento de dados.

3.55 Permitir monitoramento das atividades de processamento de dados.

3.56 Permitir sinalizar riscos relacionados com envolvimento de dados confidenciais e sensíveis.

3.57 Permitir criação de modelos padrão de processamento de dados a partir das descobertas realizadas.

3.58 Permitir carregamento manual dos modelos de processamento de dados.

3.59 Permitir descobrimentos de compartilhamento de dados com terceiros.

3.60 Permitir documentação de compartilhamento de dados com terceiros.

3.61 Permitir geração de relatórios de processamento de dados.

3.62 Permitir geração de relatórios de compartilhamento de dados com terceiros.

3.63 Permitir avaliação de risco dos processos de negócios.

3.64 Permitir gestão da conformidade com regulamentações.

3.65 Permitir revisão e aplicação das recomendações sobre processos de negócio para agilizar a documentação.

3.66 Permitir exportação da documentação dos processos em formato PDF, ou semelhante.

3.67 Permitir mapear e documentar fluxos de risco de privacidade.

3.68 Permitir mapear e documentar a estrutura organizacional de privacidade.

3.69 Permitir avaliação de risco relacionado aos terceiros.

3.70 Permitir colaboração na avaliação de risco.

3.71 Permitir medição níveis de acessos e exposição pública.

3.72 Permitir documentação das transferências de dados.

3.73 Alterar em função de acionamento dos gatilhos de nível de risco.

3.74 Permitir gestão de fluxos de trabalho de correção de dados (remediação).

3.75 Oferecer as trilhas de auditoria e relatórios.

ITEM 4 – MÓDULO DE SEGURANÇA DE DADOS

4. Características Gerais

4.1 Permitir correção dos conjuntos de dados com violações e problemas, com orquestração de fluxo de trabalho.

4.2 Priorizar as descobertas por sensibilidade e nível de risco de exposição.

4.3 Permitir atribuir a usuário atividade de correção relacionada com conjuntos de dados.

4.4 Permitir delegar as atividades de correção por função, escopo e usuário.

4.5 Permitir automação de ações de remediação como deleção, quarentena por API.

4.6 Permitir coleção de informações para trilha de auditoria das ações tomadas.

4.7 Permitir colaboração entre as equipes e comentários.

4.8 Permitir integração com ferramentas terceiras para anonimização, criptografia, aposentadoria etc.

4.9 Permitir definição de SLA para ações de remediação.

4.10 Permitir atribuição de pontuações de risco com base na fonte de dados.

4.11 Permitir atribuição de pontuações de risco por tipo de dados (classificação de atributos).

4.12 Permitir atribuição de pontuações de risco por país de residência do titular.

4.13 Informar o fator de risco de acordo com qualquer critério escolhido pelo usuário (organização, sistema, atributo, entidade etc.).

4.14 Permitir identificação dos usuários e contas com privilégios excessivos.

4.15 Permitir identificação dos dados superexpostos por sensibilidade.

4.16 Fornecer a visibilidade de acessos no nível interno e externo, por sensibilidade.

4.17 Sinalizar e permitir investigação dos problemas de alto risco.

4.18 Integrar para o catálogo os objetos com acessos ou permissões excessivas.

4.19 Permitir identificação de dados regulamentados superexpostos.

4.20 Permitir identificação e monitoramento contínuo de dados confidenciais superexpostos.

4.21 Permitir identificação dos usuários com privilégios excessivos.

4.22 Permitir identificação de dados sensíveis duplicados (superfície de ataque).

4.23 Permitir revogar privilégios excessivos e/ou automatizar este processo.

4.24 Permitir integração com ferramentas DLP para reforçar o cumprimento.

4.25 Permitir etiquetação dos objetos de acordo com classificação de sensibilidade.

4.26 Permitir etiquetação dos objetos de acordo com tipo de documento.

ITEM 5 – GESTÃO DE ATENDIMENTO

5. Características Gerais

5.1 Possuir em sua plataforma uma aplicação de Gerenciamento de Serviços a contratantes internos e externos do CONTRATANTE, a qual possui como foco atender aos usuários de uma forma avançada e com qualidade.

5.2 Possuir funcionalidade que permita construir (customizar) de forma *no code/low code* portais customizados por tipo de CONTRATANTE ou cidadão.

5.3 Possuir um modelo de dados centralizado e integrado baseado em nuvem com CMDB nativo.

5.4 Permitir suporte para desenvolvedores *no-code, low-code e pro-code*.

5.5 Possuir ambiente, permitindo que os atendentes do telefone, o portal, o chat e a interação por e-mail sejam feitos pela mesma aplicação.

5.6 Permitir automatizar tarefas redundantes para o CONTRATANTE, por meio do *Chatbot*.

5.7 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.

5.8 Possuir a funcionalidade de forçar perfis mandatório para atendimento de casos que exigem esse tipo de perfil profissional.

5.9 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.

5.10 Fornecer alertas aos agentes e fazer a linha de tempo de interação com o CONTRATANTE/solicitante.

5.11 Possuir uma camada de colaboração avançada para suportar as comunicações da equipe.

5.12 Fornecer notificações proativas de suporte via e-mail, SMS e portal para os contratantes afetados.

5.13 Possuir 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.

5.14 Fornecer autoatendimento personalizado por meio de um portal de serviços configurável que incorpora uma base de conhecimento, catálogo de serviços e comunidades.

5.15 Ser capaz de conectar outros departamentos aos processos de atendimento ao contratante em uma única plataforma com aderência interna aos níveis mínimos de serviços.

5.16 Deve ser capaz de suportar diferentes SLA's para diferentes produtos pertencentes a um contratante.

5.17 Permitir totalmente SLA's para objetos diferentes do objeto "caso", como em tarefas, incidentes, problemas, alterações e solicitações associados a um caso.

5.18 Fornecer gerenciamento de solicitações com várias camadas e permitir o relacionamento com registros de incidente, problemas e outras solicitações de serviço.

5.19 Fornecer escalonamento automático sem intervenção manual.

5.20 Fornecer *chatbot* ou agente virtual que permita o desenvolvimento de diálogos conversacionais.

5.21 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*.

5.22 Exibir no espaço de trabalho do agente 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.

5.23 Permitir o feedback do contratante sobre o artigo da base de conhecimento, por meio de um processo estruturado e automatizado de feedback.

5.24 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.

5.25 Permitir na gestão do conhecimento, 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.

ITENS 6 E 7 – SOLUÇÃO DE TESTE DE PENETRAÇÃO

6. Características Gerais

6.1 Possibilitar integração com outras ferramentas para replicar detecções de ransomware para que seja possível isolar o ataque, criptografar para gerar um mapa de ataques de ransomware.

6.2 Simular ou emular ransomware para testar em ambiente Windows.

6.3 Rodar um escopo de teste em intervalos de endereços IPs e deve permitir a exclusão de um único host ou qualquer serviço dentro do host.

6.4 Permitir ser parado a qualquer momento para que não ocorra um impacto na infraestrutura computacional.

6.5 O teste de penetração deve possuir níveis diferenciados, com no mínimo 3 níveis de varreduras.

6.6 Realizar varreduras de vulnerabilidades classificadas como críticas para uma ação rápida de resolução.

6.7 Possuir formas de teste direcionado, teste de ação única para um *report* rápido sobre determinado host ou serviço.

6.8 Possuir função de higienização automática para limpar qualquer resíduo do teste executado.

6.9 Possuir um escopo específico para o Active Directory para identificar vulnerabilidades em tempo real, referente a usuários, grupos e contas administrativas.

6.10 Ter a cobertura mínima do OWASP top 10, incluindo JAVA/ASP e RCE.

6.11 Possuir uma forma de validação por um gestor ou usuário específico, para dar maior visibilidade e transparência no processo de ataque.

6.12 Identificar uma vulnerabilidade em um escopo de teste e versionar as atualizações para executar um processo completo de controle de qualidade.

6.13 Possuir funcionalidade de interceptar comunicações entre duas partes e retransmitir os dados para outro dispositivo (de terceiros), incluindo técnicas baseadas em rede MITM.

6.14 Possuir algumas medidas para recuperar senhas em texto simples de usuários, hosts e servidores, quebrando *hashes* de senhas de dados armazenados ou transportados de um sistema usando uma das seguintes

combinações de técnicas de força bruta e dicionário:

6.14.1 Uso de senha padrão do fabricante em dispositivos periféricos;

6.14.2 Validar a existência de senhas fracas;

6.14.3 Verifique a robustez das senhas mais complexas e teste se elas estão de acordo com a política corporativa;

6.14.4 Use recursos de *cracking* baseados em hardware para detectar falhas no ecossistema *Kerberos*;

6.14.5 Teste a força da senha de contas privilegiadas em endpoints não gerenciados;

6.14.6 Aproveite o poder de computação de GPU especializado para técnicas de *cracking* de alto desempenho;

6.14.7 Dicionário de senhas onde o sistema aplicará automaticamente as transformações;

6.14.8 Crie um dicionário personalizado de senhas para caçar.

ITEM 8 – SOLUÇÃO DE ANONIMIZAÇÃO / CRIPTOGRAFIA

7. Características Gerais

7.1 Fornecer APIs e Agentes que permitam a criptografia de arquivos, mascaramento estático e dinâmico, anonimização, pseudonimização de dados pessoais e dados sensíveis.

7.2 Fornecer agentes de promovam a criptografia para dados estruturados e não estruturados para dados em repouso com gerenciamento centralizado de chaves, controle de acesso de usuários, incluindo usuários privilegiados, e registro detalhado de auditoria de acesso visando atender aos requisitos de conformidade e práticas recomendadas para proteger os dados, onde quer que estejam. Os agentes deverão residir no sistema operacional, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela.

7.3 Os agentes devem possuir certificação FIPS 140-2 Nível 1 e devem permitir a criptografia ou rotação de chaves sem bloquear o acesso de usuários ou de aplicativos aos dados em questão, ou seja, sem indisponibilidade nos serviços. Rotação de chaves significa descriptografar os dados com a chave criptográfica atual e criptografá-los com uma nova chave criptográfica.

7.3.1 Permitir o consumo de APIs e instalação de agentes nos seguintes sistemas operacionais:

a. Linux 64 bits;

b. Microsoft Windows 64 bits.

7.4 Permitir a integração com sistemas de banco de dados ORACLE e Microsoft SQL Server, permitindo o uso de funções criptográficas em comandos SQL.

7.5 Permitir, via REST API, a 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.

7.6 Permitir a pseudonimização dos dados de forma que os dados do titular não possam ser identificados, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

7.7 Permitir o compartilhamento/replicação segura(o), com funcionamento baseado em tabela e/ou coluna e utilizando as operações de criptografia / Toquenização e descriptografia / destoquenização , de bases de dados heterogêneas com suporte a pelo menos arquivo CSV, Microsoft SQL Server, MySQL e Oracle.

7.8 Garantir que o processo de pseudonimização garanta a proteção dos dados originais através da criptografia de dados com algoritmo AES-256 para a geração de um BLOB (*Binary Large Object*).

7.8.1 Possuir função para a geração do Token (representação visual do dado original, com preservação de formato;

7.9 A API deverá ter funções de cálculo de resumo de dados (HASH), nos seguintes padrões:

7.9.1 MD5;

7.9.2 SHA1;

7.9.3 SHA2 de 224, 256, 384 e 512 bits;

7.10 Permitir a 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.

7.11 Permitir a pseudonimização dos dados de forma que os dados do titular não possam ser identificados, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

7.12 Permitir armazenamento e gerenciamento de chaves criptográficas em ambiente seguro e certificado FIPS 140-2 nível 1 ou superior em alta disponibilidade.

7.12.1 O ambiente de armazenamento e gerenciamento de chaves deverá possuir integração com SIEM – sistemas de gerenciamento de ogs do mercado, como: Splunk, qRadar, Arcsight, McAfee, LogRhythm e etc;

7.12.2 Todo o processamento criptográfico deverá ocorrer neste ambiente certificado, sem a necessidade de transporte da chave para ambiente externo.

7.12.3 As chaves deverão ser acessíveis, via os seguintes métodos:

a. Protocolo PKCS#11;

b. REST API;

c. Protocolo KMIP.

7.13 A solução deverá permitir, além do processamento de tokenização, o uso de algoritmos criptográficos de uso genérico, sendo exigidos, pelo menos os listados abaixo:

7.13.1 3 DES;

7.13.2 AES-128;

7.13.3 AES-256;

7.13.4 ARIA128;

7.13.5 ARIA256;

7.13.6 RSA-1024;

7.13.7 RSA-2048;

7.13.8 RSA-4096.

7.14 Possuir capacidade para controlar o acesso a chaves criptográficas utilizadas no processo de tokenização de dados.

7.15 Ser licenciada para cobrir, pelo menos, 10 (dez) sistemas de banco de dados, 5(cinco) servidores de aplicação e 5(cinco) servidores de arquivos sem limites de uso com relação as funcionalidades indicadas neste item.

LOTE 2 - DESCRITIVO SERVIÇOS ESPECIALIZADOS

ITEM 1 – SERVIÇO DE IMPLANTAÇÃO DO ITEM 1 DO LOTE 1:

8. Características Gerais

8.1 A CONTRATADA deverá realizar todas as parametrizações, customizações e adaptações necessárias ao pleno funcionamento operacional da solução.

8.2 A CONTRATADA deverá realizar, para dados estruturados, o *data Discovery*, integração com portal do titular e gestão jurídica (*Data Mapping*), seguindo a Política de Gestão e Governança de Dados Corporativo da CONTRATANTE, considerando todas as bases de dados utilizados pela CONTRATANTE, devendo gerar as seguintes informações:

8.2.1 *Dashboard* com o resultado do *Data Discovery* informando quantidade de banco de dados por tecnologia;

8.2.2 *Dashboard* com o resultado do inventário de servidores analisados (Discos, memória, Ethernet etc.);

8.2.3 *Dashboard* com o resultado do *Data Discovery* por banco de dados, informando quais bancos de dados possuem dados pessoais e/ou sensíveis e a quantidade de colunas que contêm cada dado em cada banco de dados.

8.3 A CONTRATADA deverá realizar, para dados não estruturados, o *data discovery*, *data mapping*, integração com portal do titular, seguindo a Política de Gestão e Governança de Dados Corporativo da CONTRATANTE, considerando todas os repositórios de dados não estruturados utilizados pela CONTRATANTE, devendo gerar as seguintes informações:

8.3.1 *Dashboard* com o resultado do *Data Discovery* informando quantidade de documentos com dados pessoais e/ou sensíveis;

8.3.2 Permitir criar gráficos e relatórios com o resultado do *Data Discovery*;

8.3.3 *Dashboard* com o resultado do *Data Discovery* por repositório, informando quais diretórios/servidores possuem dados pessoais e/ou sensíveis e a quantidade de dados por tipo (CFP, RG, NOME etc.).

8.4 As integrações deverão ser sugeridas pela CONTRATADA, permitindo que a CONTRATANTE possa estruturar papéis necessários para gestão de informações; definição da estratégia de dados das áreas de negócio; cesta de indicadores que permita:

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

8.4.2 Medir qualidade das informações;

8.4.3 Eficiência e eficácia dos processos de governança e gestão dedados;

8.4.4 Engajamento das áreas de negócio e TI.

ITEM 2 – SERVIÇOS DE IMPLANTAÇÃO DOS ITENS 2, 3, 4, 5, 6 / 7 e 8 do LOTE 1:

9. Características Gerais

9.1 Esse serviço se prestará para a implantação dos itens 1.2, 1.3, 1.4, 1.5, 1.6 e 1.8, devendo ser iniciados mediante requisição da CONTRATANTE através de Ordem de Serviço (OS) específica para esse fim.

9.2 Deverão ser executados todos os serviços de parametrização, customização e integração, necessários ao pleno funcionamento de cada módulo em suas funcionalidades nativas.

9.3 Após a implantação de cada módulo, a CONTRATADA deverá realizar avaliação no ambiente computacional da CONTRATANTE, a fim de, consultivamente, sugerir melhorias no uso das soluções e alertas quando o nível de processamento demonstrar risco de saturação presente ou futura.

9.4 A CONTRATADA deverá apoiar consultivamente os times de bancos de dados e sistemas da CONTRATANTE para que os níveis adequados segurança, gestão, de criptografia, mascaramento de dados e tokenização sejam implementados sem que haja degradação de performance ou comprometimento no ambiente da CONTRATANTE.

9.5 A CONTRATADA deverá manter todas os dados e informações da CONTRATANTE de forma segura e sigilosa, como as chaves criptográficas, que deverão ser armazenadas de forma segura no ambiente da CONTRATANTE, em local centralizado e com acesso restrito apenas a pessoal autorizado designado da CONTRATANTE.

9.6 Deverá ser efetuado, ainda no processo de implantação, um treinamento de cada solução, para até 5 (cinco) pessoas, abordando seus conceitos e funcionalidades básicas.

9.7 A CONTRATADA deverá propor duração e conteúdo de cada treinamento, que deverá ser aprovado pela CONTRATANTE.

9.8 As instalações/disponibilizações deverão seguir os seguintes critérios:

9.8.1 Deverá ser disponibilizado um ambiente de desenvolvimento e/ou homologação para instalação do cliente, caso haja, e demonstração do seu funcionamento para equipe técnica da CONTRATANTE;

9.8.,2 As soluções deverão ser instaladas/disponibilizadas e configuradas de forma redundante, em alta-disponibilidade.

9.9 Para o item 1.8 – Solução de Anonimização/Criptografia:

9.9.1 Todos os procedimentos de segurança deverão ser levados em consideração na configuração da solução, incluindo a aplicação de filtros de acesso ao processamento e gerência da solução.

9.9.2 Para o processo de homologação, deverão ser instalados, pelo menos 1 servidor de desenvolvimento, 1 servidor de arquivos e 1 servidor de banco de dados integrados com o ambiente centralizado de armazenamento de chaves criptográficas e processamento criptográfico.

9.9.3 O fornecedor da solução poderá fazer toda a instalação dirigida, remotamente, com a disponibilização de profissional qualificado durante um período de, pelo menos, 80 horas para a instalação/setup remoto.

9.9.4 O suporte deverá ser provido no formato remoto, durante o horário comercial, ou seja, na modalidade 8x5.

9.9.5 O tempo de resposta deverá atender aos seguintes critérios:

a. Dúvidas devem ser respondidas em até 48 horas;

b. Eventos que influenciem em performance ou mal funcionamento, mas sem impacto crítico deverão ser respondidos em até 8 horas;

c. Eventos que impactem, diretamente, no funcionamento da solução, deverão ser atendidos em até 4 horas;

d. Eventos que impeçam o funcionamento ou que tenha grave impacto no funcionamento, deverão ser atendidos em até 2 horas.

9.10 Os serviços de suporte, manutenção e garantia deverão ter duração de 12 (doze) meses.

ITEM 3 – SERVIÇO DE HOSPEDAGEM EM NUVEM

10. Características Gerais

10.1 A CONTRATANTE deverá contar com uma disponibilidade de acesso 24 horas por dia, sete dias por semana. As políticas e a modalidade de acesso deverão ser especificadas em um manual de acesso ou documento de boas-vindas do *Data Center*.

10.2 O serviço de *Colocation* deverá prever as seguintes modalidades: *mini rack*, *full rack*, e *cage*. A CONTRATANTE poderá optar pela modalidade que melhor se ajuste às suas necessidades de negócio.

10.3 Condições de Construção Predial

10.3.1 As instalações dos *Data Centers* têm características definidas na sua construção para evitar ou minimizar os riscos de origem geológica e/ou meteorológica, contando com instalações em áreas que possam ter terremotos, ou contra furacões em áreas que cuja presença de furacões é frequente.

10.4 Fornecimento de Energia Elétrica Garantida

10.4.1 A CONTRATADA deverá ter o sistema de energia projetado de forma a garantir uma alta disponibilidade, tornando quase impossível a interrupção do serviço, ou mesmo a degradação da qualidade do serviço por falha no sistema. Não deverá existir qualquer ponto único de falha que possa interromper o fornecimento de energia para o ambiente dos equipamentos.

10.4.2 O *Data Center* da CONTRATADA deverá possuir um sistema completo de energia em redundância 3N+1. Toda a infraestrutura deverá ser dimensionada para que não haja nenhuma degradação do serviço, mesmo com a falha de um componente. A Redundância N+1 deverá ser aplicada aos geradores, retificadores, ar condicionado, *no-breaks* e alimentação elétrica, formando dois sistemas redundantes em paralelo. Entre os geradores e os racks deverão existir no mínimo 2 (dois) circuitos elétricos totalmente independentes.

10.4.3 Todos os componentes rotativos (motores e geradores) e outras eventuais fontes de interferência eletromagnética deverão estar localizados em um edifício afastado do prédio de equipamentos. A subestação da CONTRATADA deverá ter a energia fornecida pela concessionária em média em 13.800 Volts com proteção e seccionada com disjuntores classe 15KV, isolamento SF6, relés de proteção secundária estáticos e transformadores de no mínimo 750 KVA, funcionando em configuração redundante n+1.

10.4.4 A infraestrutura de distribuição em baixa tensão deverá ser do tipo TN-C com 5 condutores (3 fases + neutro + terra), possuindo um barramento “não essencial” para as instalações prediais de uso de escritório, um barramento “essencial” ligado ao sistema de geração próprio e um barramento “crítico” (*no break*) ligado ao Sistema de UPS. A energia em baixa tensão deverá ser fornecida aos racks em 120V AC, podendo também ser fornecida em 220V AC ou 48V DC, conforme especificado pela CONTRATANTE.

10.4.5 O *Data Center* da CONTRATADA deverá ter os sistemas de proteção e monitoramento de energia analisam permanentemente o estado de diversos parâmetros, tais como, consumo de corrente, tensão e fator de potência, podendo também ser monitorados remotamente. A automação deve ser realizada por um controle lógico inteligente com análise de demanda.

10.4.6 O sistema próprio de geração de energia deverá dispor de grupos geradores de no mínimo 450 KVA cada, operando em paralelo e com unidades de supervisão (USCA) microprocessadas, com redundância N+1.

10.4.7 O sistema de combustível Diesel deverá ser composto por 1 tanque de grande capacidade que bombeia o óleo para tanques intermediários menores, usados para armazenamento de consumo e destes para tanques de pequena capacidade, para armazenamento técnico de cada grupo gerador.

10.4.8 O sistema de geradores deve ter autonomia para aproximadamente 7 dias sem reabastecimento, podendo ser reabastecido em carga. Convênios com distribuidoras de diesel, garantem a continuidade ilimitada da disponibilidade de energia elétrica.

10.4.9 O Sistema de “*No Break*” (UPS) deverá ser composto por, no mínimo, equipamentos Powerware de última geração em ligação 1+1 e com barramento interligado. Os UPS funcionam em modo “*on line*” contínuo, de forma a não provocar transientes.

10.4.10 A proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento devem seguir os padrões ETSI, ITU-T e NBR 113. O aterramento deve atender às recomendações ITU-T K-27. Todos os “*cable trays*”, “*racks*” e gabinetes deverão ser aterrados. O sistema de administração redundante da energia elétrica dos *Data Centers* deverá fornecer potência limpa e independente a CONTRATANTE e sistemas críticos. O Sistema de *No-Breaks* deverá consistir em sistemas múltiplos de *No-Breaks*. Caso um falhe, os demais podem assumir a carga sem exceder sua capacidade nominal. As baterias do *No-Break* deverão ser carregadas pela rede pública de energia elétrica ou pelos geradores redundantes de reserva nos *Data Centers*.

10.4.11 Os *Data Centers* deverão ser alimentados por transformadores dedicados e redundantes. O serviço entrante deverá ser respaldado e sustentado por painéis automáticos de transferência e geradores a diesel redundantes que verificam a qualidade da energia ou interrupções.

10.4.12 As cargas elétricas deverão ser alimentadas por sistemas de *No-Breaks* paralelos e redundantes que são configurados como *bridge* estática automática e com circuitos de derivação manuais. Cada módulo de *No-Break* deverá ter seu próprio grupo de baterias com capacidade suficiente para manter a carga elétrica dos Datacenters por período mínimo de 30 minutos, e ser tempo suficiente para a entrada em operação de geradores a diesel, que deverão requerer até um minuto para a sua estabilização.

a. Em cada um dos *Data Centers*, deverão ter *turbog* geradores a diesel capazes de entrar em operação e se acoplarem automaticamente à rede elétrica em um minuto. Esses geradores deverão ter tanques de combustível que permitirá sua realimentação externa, facilitando uma operação contínua com grande autonomia. Os geradores deverão contar com

sistemas automáticos para que, após a inicialização, permaneçam em funcionamento somente o(s) gerador(es) que corresponda(m) à capacidade de energia demandada.

b. Deverá atender aos padrões de conexão conforme especificações e recomendações pelas normas ITU-T K-27 e ETS1.

c. Cada *rack* ou *mini-rack* deverá ser alimentado por no mínimo dois PDUs, que são utilizados para melhorar a redundância dos equipamentos que possuem dupla fonte ou entrada de energia.

10.5 Sistema Anti-Incêndio

10.5.1 O sistema da supressão de incêndios nos *Data Centers* da CONTRATADA deverá contar com sistema de detecção antecipada, que detecta a fumaça nas primeiras etapas da combustão por meio de um analisador de gases baseado em um raio laser que inspeciona a composição do ar dentro do *Data Center*. Este sistema de detecção deverá ser respaldado por sistemas iônicos de detecção de partículas.

10.5.2 Caso um sistema de detecção de incêndio for acionado, os *Data Centers* deverão contar com um sistema de extinção redundante contra incêndios por meio da utilização de Gás FM200 ou similar mais moderno.

10.6 Sistema de Controle Ambiental e Ar-Condicionado

10.6.1 Os *Data Centers* da CONTRATADA deverão contar com um sistema de refrigeração baseado em equipamentos MCU (Modular *CoolingUnits*), que recebem o fluido refrigerado e insuflam ar refrigerado por baixo do piso elevado, forçando a saída do mesmo pela parte superior de cada *rack*. A infraestrutura deverá oferecer diversas unidades de ar-condicionado que irão assegurar uma adequada dissipação de calor. Caso uma unidade de ar-condicionado falhe, as outras unidades deverão compensar a carga térmica completa dos equipamentos alojados.

10.6.2 A CONTRATADA deverá manter sempre múltiplas unidades MCU nos Datacenters, e elas deverão ser alimentadas pela rede de energia garantida para assegurar a continuidade das operações. Estas ainda deverão ser monitoradas por meio de um sistema de gerência – tipo SCADA, que permite a gestão e controles adequados para a detecção de qualquer falha. A temperatura nos *Data Centers* deverá ser mantida entre 17 e 27ºC. A umidade relativa dos *Data Centers* da CONTRATADA deverá ser controlada para que ela se mantenha sempre entre 40-60%, não permitindo desta forma a condensação.

10.6.3 A CONTRATADA deverá ter um processo de verificação permanente do ar na sala de equipamentos, onde deverá ser possível detectar a presença de fumaça, estado dos filtros de pó, diferença de temperatura etc.

10.6.4 A CONTRATADA deverá ter a infraestrutura dos equipamentos de refrigeração e controle configurados para atender ao esquema mínimo de redundância 2N+1.

10.7 Controle de Acessos

10.7.1 A segurança de cada *Data Center* deve ser mantida por um sistema de vigilância por circuito fechado de televisão digital, alarmes de movimento e pessoal 24 horas por dia.

10.7.2 Devem existir câmeras de monitoramento montadas dentro e fora de cada edifício. A vigilância deve ser monitorada localmente em cada local. As informações registradas nas câmeras devem ser mantidas em meios magnéticos para posterior análise em caso de necessidade.

10.7.3 Os *Data Centers* devem exigir uma identificação biométrica ou cartão de proximidade, que permita o acesso às diferentes áreas e salas. Estas devem ser habilitadas pela CONTRATADA, utilizando tecnologia de última geração (*scanners* portáteis, leitores de impressão digital etc.).

10.7.4 O controle de acesso às áreas de *Colocation* deve ser realizado de forma rígida, e concedido apenas às pessoas autorizadas pela CONTRATANTE para este fim.

10.8 Suporte

10.8.1 A CONTRATADA deve contar com Centros de Operação e monitoramento que funcionam 7X24 horas e devem ser responsáveis pela manutenção da infraestrutura que suporta a operação dos *Data Centers* e oferecer ajuda imediata frente a qualquer eventualidade.

10.8.2 Ao mesmo tempo, oferecer equipamentos e peças redundantes em cada local para suportar substituições de emergência, e acordos com cada fornecedor dos serviços de infraestrutura, visando assegurar a continuidade da operação dos *Data Centers*.

10.9 Segurança da Informação

10.9.1 O Ambiente de computação em nuvem deve fornecer uma segurança da informação por WAF (*Web Application Firewall*) para proporcionar uma melhor segurança e monitoramento de tráfego HTTP nos serviços hospedados.

10.10 Manutenção

10.10.1 Rotinas de manutenção periódicas devem ser realizadas em todas as instalações.

10.10.2 Para o desenvolvimento das tarefas de manutenção, a CONTRATADA considerará as recomendações e procedimentos fornecidos pelos diferentes fornecedores de dispositivos e infraestrutura, visando garantir o cumprimento dos seus respectivos requisitos operacionais.

ITEM 4 – SERVIÇOS DE CUSTOMIZAÇÃO E DESENVOLVIMENTO DE INTEGRAÇÕES

11. Características Gerais

11.1 Todos os serviços serão demandados pela SEAD-PI através de Ordens de Serviço (OS), sob demanda e mensurados em Unidades de Serviço Técnico (UST), conforme regras e Níveis de Serviço definidos no Termo de Referência (TR).

11.2 AS OSs conterão todos os parâmetros necessários à sua execução, controle e gestão dos serviços a serem prestados, como escopo, prazo, estimativa de USTs, entre outros.

11.3 Os Serviços Técnicos Especializados atenderão a diferentes demandas por parte da SEAD-PI, como consultoria e customização das soluções.

11.4 Todos os serviços demandados deverão ser previamente planejados, com devido Plano de Trabalho elaborado pela CONTRATADA e aprovado pela SEAD-PI.

11.5 Deverão ser executados de forma a garantir o pleno funcionamento das soluções de forma a atender aos requisitos identificados de forma integrada ao ambiente informacional da SEAD-PI.

11.6 Os métodos de acesso e integração às bases de dados da SEAD-PI deverão ser propostos pela CONTRATADA e devidamente apresentada, discutida e aprovada junto as áreas técnicas da SEAD-PI responsáveis pelas áreas de Banco de Dados e Segurança.

ITEM 5 – SERVIÇO DE MAPEAMENTO E ANÁLISE DE PROCESSOS DE NEGÓCIO

12. Características Gerais

12.1 Todos os serviços serão demandados pela SEAD-PI através de Ordens de Serviço (OS), sob demanda e mensurados em Unidades de Serviço Técnico (UST), conforme regras e Níveis de Serviço definidos no Termo de Referência (TR).

12.2 AS OSs conterão todos os parâmetros necessários à sua execução, controle e gestão dos serviços a serem prestados, como escopo, prazo, estimativa de USTs, entre outros.

12.3 Os Serviços Técnicos Especializados atenderão a diferentes demandas por parte da SEAD-PI, como consultoria e customização das soluções.

12.4 Todos os serviços demandados deverão ser previamente planejados, com devido Plano de Trabalho elaborado pela CONTRATADA e aprovado pela SEAD-PI.

12.5 O objetivo desse serviço é o de identificar e rastrear os dados pessoais utilizados nos processos de negócio e seu tratamento de privacidade.

12.6 A identificação dos processos de negócio e mapeamento dos dados pessoais, é o primeiro passo para diagnosticar sua conformidade com relação à LGPD.

12.7 Deverá ser entregue a relação dos processos de negócio que coletam, manipulam e tratam dados pessoais, diagnóstico de sua conformidade ou não à legislação e, medidas/ações de mitigação/adequação dos não conformes.

ITEM 6 – TRANSFERÊNCIA DE CONHECIMENTO

13. Características Gerais

13.1 Com o objetivo de alinhamento às recomendações relacionadas à COVID-19, de evitar aglomeração em eventos onde o comparecimento presencial não seja fundamental, os eventos de treinamento e capacitação deverão ser executados de forma **Remota**.

13.2 Deverá ser elaborado, em acordo entre as partes, CONTRATANTE e CONTRATADA, um **Plano de Treinamento e Capacitação** que garanta a fluidez no início de operação da solução e, também, a independência da SEAD-PI em relação à CONTRATADA e consequente continuidade operacional após o término da execução contratual.

13.3 A princípio, mesmo a solução a ser contratada sendo na modalidade SaaS, entendemos que serão necessários 2 (dois) tipos de treinamento que capacite os diferentes perfis na plena operação da solução, sendo os perfis: Usuário Final e Administrador/Implementador.

13.4 A(s) ementa(s) do(s) treinamento(s) deverá(ão) ser elaborada(s) pela CONTRATADA e aprovada(s) pela SEAD-PI.

13.5 O treinamento deverá ser composto de parte teórica e parte prática, cobrindo o dia-a-dia que cada perfil de usuário encontrará na operação da solução.

13.6 O ambiente para o treinamento e execução dos exercícios práticos deverá ser exatamente o mesmo em termos de configuração e interface, que o usuário utilizará no ambiente produtivo.

13.7 Deverá ser disponibilizado para cada treinando, material impresso e/ou digital de apoio ao treinamento e eventual consulta futura pelo usuário, como Ajuda, Guias Rápidos, Apostilas etc., todos em língua Portuguesa do Brasil.

13.8 Cada treinamento não deverá exceder o total de 6 (seis) horas para o perfil Usuário Final e 18 (dezoito) horas para Administrador/implementador, devendo ser ministrado em períodos não superiores a 3 (horas) diárias e 9 (nove) horas semanais.

13.9 A CONTRATADA deverá elaborar uma avaliação do treinamento junto aos treinandos, que deverá ser aprovada pela SEAD-PI, cobrindo os principais aspectos como capacidade e comunicação do instrutor, conteúdo programático, atingimento dos objetos, entre outros, com avaliação de 1 a 10 nos itens elencados.

13.10 A SEAD-PI só considerará o treinamento concluído com sucesso, com os consequentes atesto final e respectivo pagamento, caso a avaliação média obtida juntos aos treinandos seja igual ou superior a nota 8 (oito). Caso contrário, a CONTRATADA deverá resolver os problemas apontados e repetir o treinamento, sem custos adicionais para a SEAD-PI.

ITEM 7 – ACESSO À PLATAFORMA EAD PARA SEGURANÇA DA INFORMAÇÃO

14. Características Gerais

14.1 A Plataforma de Educação à Distância deverá disponibilizar diferentes tipos de treinamento voltados ao tema Segurança da Informação, com diferentes trilhas e níveis de complexidade, de forma a possibilitar da introdução à especialização no referido tema.

14.2 O acesso a Plataforma deverá ser por licença concorrente, de forma a possibilitar uma melhor distribuição e uso da Plataforma, sem vincular o acesso a servidores específicos.

14.3 Deverá ser fornecido diferentes mídias na exposição, como textos, áudios e vídeos.

14.4 Deverá ser possível a interrupção e posterior continuação a critério do usuário.

14.5 Deverá existir alguma forma de verificação do aprendizado.

14.6 A Plataforma deverá oferecer diferentes tipos de relatórios com relação à sua utilização e aproveitamento dos alunos, de forma a oferecer aos gestores subsídios para avaliar a efetividade da iniciativa.

14.7 Deverá ser permitido ao usuário a obtenção de algum certificado ou comprovação de conclusão dos cursos realizados.

ANEXO III DO TERMO DE REFERÊNCIA

FORMULÁRIO DE AVALIAÇÃO DA PROVA DE CONCEITO

Na ocasião da POC, a equipe técnica irá considerar apto o sistema que atender os seguintes requisitos:

Item	Requisito a ser Observados no Teste de Bancada	Atende (Sim/Não)
1	Apresentar integração e descoberta de dados (data Discovery) com repositório de dados estruturados, com todas as seguintes fontes de dados: ADABAS, Oracle, MSSQL, MySQL e MongoDB.	
2	Demonstrar que a plataforma web, atende todos os requisitos preconizados pela LGPD, relacionados aos gerenciamentos listados a seguir:	
2.1.	Gerenciamento de Requisições do Titular e Portal de Serviços;	
2.2.	Gerenciamento de Incidentes;	
2.3.	Gerenciamento de Bases Legais, Políticas e Termos;	

2.4.	Gerenciamento de Terceiros;	
2.5.	Gerenciamento de Dados não Estruturados;	
2.6.	Gerenciamento de Dados Estruturados e Inventário de Ativos de Dados Pessoais;	
2.7.	Gerenciamento de Indicadores da LGPD;	
2.8.	Gerenciamento de Capacitação da LGPD;	
2.9.	Gerenciamento de Análise Jurídica.	
3	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 ou O365.	
4	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.	
5	Apresentar a funcionalidade de geolocalização da informação/fonte de dados classificado e "mapa de calor" dos sistemas com mais dados pessoais e sensíveis.	
6	Demonstrar a capacidade de mapeamento automático de dados entre sistemas diferentes, realizando uma “conexão” gráfica entre estes sistemas.	
7	Demonstrar a capacidade de encontrar atributos não mapeados ou configurados na ferramenta para busca.	
8	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).	
9	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.	
10	Demonstrar a capacidade de agendamento das varreduras durante as janelas predefinidas, permitindo acompanhá-las, iniciar, pausar, e parar uma varredura manualmente.	
11	Demonstrar que a ferramenta conta com, minimamente, as seguintes expressões regulares nativamente (e com validação/checksum, onde aplicar): 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.	
12	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).	
13	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.	
14	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.).	

15	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.	
16	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.	
17	Demonstrar acionabilidade das políticas infringidas, notificando o responsável do sistema afetado e a capacidade de acionamento automático de ferramentas terceiras por API.	
18	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).	
19	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.	
20	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.	
21	Demonstrar a capacidade de acionamento e alertas dos responsáveis para violações de políticas de qualidade.	
22	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.	
23	Demonstrar a definição de políticas de retenção legal (dados que não devem ser excluídos apesar que cumprirem prazos de ciclo de sua vida).	
24	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.	
25	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.	
26	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.	
27	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.	
28	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.	
29	Demonstrar a emissão de relatório de acesso aos dados do titular (dossiê) a permitir da requisição e obtenção do dossiê através de API.	

30	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.	
31	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.	
32	Demonstrar as notificações automáticas por e-mail informando ao titular solicitante os avanços no atendimento da sua solicitação.	
33	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.	
34	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.	
35	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.	
36	Demonstrar a capacidade de identificação de dados sensíveis expostos aos usuários externos ou compartilhados publicamente.	
37	Demonstrar a integração com ferramentas DLP como MIP, para reforçar a proteção de objetos de dados de acordo com níveis de sensibilidade.	
38	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.	
39	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.	
40	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).	
41	Demonstrar um modelo de proteção para informações de tal forma que o dado seja devidamente criptografado no sistema de arquivos.	
42	Deverá demonstrar a Tokenização e mascaramento dinâmico de dados.	
43	Demonstrar a proteção sistemas de dados estruturado (bancos de dados) e sistemas de dados não estruturado.	
44	Demonstrar a console de gerenciamento centralizado.	
45	Deverá demonstrar a integração com os sistemas de gerenciamento de logs.	
46	Deverá demonstrar que os agentes fazem a rotação/mudança de chaves sem causar indisponibilidade ou degradação nos servidores de dados.	
47	Deverá demonstrar que é capaz de ser configurada em alta disponibilidade (HA).	

48	Deverá demonstrar que os agentes instalados nos servidores operam de forma autônoma mesmo com a perda de comunicação com a console.	
49	Demonstrar que as políticas de controle de acesso podem ser aplicadas mesmo aos usuários privilegiados do sistema e estes não deverão possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio.	
50	Demonstrar o mascaramento dos dados sensíveis através da criptografia de uma determinada tabela e coluna.	

ANEXO IV DO TERMO DE REFERÊNCIA

TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES

MODELO

Processo Administrativo N°	
Processo Licitatório	
Objeto	
N° do Contrato	

A **Secretaria da Administração do Piauí**, com sede em **<local>**, inscrita no CNPJ sob o **nº 99.999.999/9999-99**, doravante denominado **CONTRATANTE** e a **Empresa** _____, estabelecida à _____, CEP: _____, inscrita no CNPJ sob o nº _____, doravante denominada simplesmente **CONTRATADA**, representada neste ato pelo Sr _____, (cargo) _____, (nacionalidade) _____, (estado civil) _____, (profissão) _____, portador da Cédula de Identidade nº _____, e do CPF nº _____, residente e domiciliado em _____, e, sempre que em conjunto referidas como PARTES para efeitos deste **TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES**, doravante denominado simplesmente TERMO, e;

CONSIDERANDO que, em razão do atendimento à exigência do Contrato Nº XX/20XX, celebrado pelas PARTES, doravante denominado **CONTRATO**, cujo objeto é a **<objeto do Contrato>**, mediante condições estabelecidas pelo **CONTRATANTE**;

CONSIDERANDO que o presente **TERMO** vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de **INFORMAÇÕES**, que a **CONTRATADA** tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do **CONTRATANTE** de que a **CONTRATADA** tomar conhecimento em razão da execução do **CONTRATO**, respeitando todos os critérios estabelecidos aplicáveis às **INFORMAÇÕES**;

O **CONTRATANTE** estabelece o presente **TERMO** mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste **TERMO** é prover a necessária e adequada **PROTEÇÃO ÀS INFORMAÇÕES** do **CONTRATANTE**, principalmente aquelas classificadas como **CONFIDENCIAIS**, em razão da execução do CONTRATO celebrado entre as

PARTES.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Parágrafo Primeiro: As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer **INFORMAÇÕES** reveladas pelo **CONTRATANTE**.

Parágrafo Segundo: A **CONTRATADA** se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer **INFORMAÇÕES** que venham a ser fornecidas pelo **CONTRATANTE**, a partir da data de assinatura deste **TERMO**, devendo ser tratadas como **INFORMAÇÕES CONFIDENCIAIS**, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo **CONTRATANTE**.

Parágrafo Terceiro: A **CONTRATADA** se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou faça uso das **INFORMAÇÕES** do **CONTRATANTE**.

Parágrafo Quarto: O **CONTRATANTE**, com base nos princípios instituídos na Segurança da Informação, zelará para que as **INFORMAÇÕES** que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela **CONTRATADA**.

CLÁUSULA TERCEIRA - DAS LIMITAÇÕES DA CONFIDENCIALIDADE

Parágrafo Único: As obrigações constantes deste **TERMO** não serão aplicadas às **INFORMAÇÕES** que:

I. Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das **PARTES**;

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 QUARTA - DAS OBRIGAÇÕES ADICIONAIS

Parágrafo Primeiro: A **CONTRATADA** se compromete a utilizar as **INFORMAÇÕES** reveladas exclusivamente para os propósitos da execução do **CONTRATO**.

Parágrafo Segundo: A **CONTRATADA** se compromete a não efetuar qualquer cópia das **INFORMAÇÕES** sem o consentimento prévio e expresso do **CONTRATANTE**.

I. O consentimento mencionado no Parágrafo segundo, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das **PARTES**.

Parágrafo Terceiro: A **CONTRATADA** se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste **TERMO** e da natureza confidencial das **INFORMAÇÕES** do **CONTRATANTE**.

Parágrafo Quarto: A **CONTRATADA** deve tomar todas as medidas necessárias à proteção das **INFORMAÇÕES** do **CONTRATANTE**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo **CONTRATANTE**.

Parágrafo Quinto: Cada **PARTE** permanecerá como única proprietária de todas e quaisquer **INFORMAÇÕES** eventualmente reveladas à outra parte em função da execução do **CONTRATO**.

Parágrafo Sexto: O presente **TERMO** não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

I. Os produtos gerados na execução do **CONTRATO**, bem como as **INFORMAÇÕES** repassadas à **CONTRATADA**, são únicas e exclusiva propriedade intelectual do **CONTRATANTE**.

Parágrafo Sétimo: A **CONTRATADA** firmará acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao **CONTRATO**, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento.

Parágrafo Oitavo: A **CONTRATADA** obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às **INFORMAÇÕES** que venham a ser reveladas durante a execução do **CONTRATO**.

CLÁUSULA QUINTA - DO RETORNO DE INFORMAÇÕES

Parágrafo Único: Todas as **INFORMAÇÕES** reveladas pelas **PARTES** permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

I. A **CONTRATADA** deverá devolver, íntegros e integralmente, todos os documentos a ela fornecida, inclusive as cópias porventura necessárias, na data estipulada pelo **CONTRATANTE** para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias.

II. A **CONTRATADA** deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais do **CONTRATANTE**, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

CLÁUSULA SEXTA - DA VIGÊNCIA

Parágrafo Único: O presente **TERMO** tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até 5 (cinco) anos após o término do Contrato.

CLÁUSULA SÉTIMA - DAS PENALIDADES

Parágrafo Único: 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** 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.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS

Parágrafo Primeiro: Este **TERMO** constitui vínculo indissociável ao **CONTRATO**, que é parte independente e regulatória deste instrumento.

Parágrafo Segundo: O presente **TERMO** constitui acordo entre as **PARTES**, relativamente ao tratamento de **INFORMAÇÕES**, principalmente as **CONFIDENCIAIS**, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas **PARTES** em ações feitas direta ou indiretamente.

Parágrafo Terceiro: Surgindo divergências quanto à interpretação do pactuado neste **TERMO** ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as **PARTES** tais divergências, de acordo com os princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa-fé, e, as preencherão com estipulações que deverão corresponder e resguardar as **INFORMAÇÕES** do **CONTRATANTE**.

Parágrafo Quarto: O disposto no presente **TERMO** prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à **CONFIDENCIALIDADE DE INFORMAÇÕES**.

Parágrafo Quinto: 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.

CLÁUSULA NONA - DO FORO

Parágrafo Único: Fica eleito o foro da **Justiça Federal - Seção Judiciária**, em Brasília - DF, para dirimir quaisquer dúvidas oriundas do presente **TERMO**, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, a **CONTRATADA** assina o presente **TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES**, em 2 (duas) vias de igual teor e um só efeito, na presença de duas testemunhas.

__, _____ de_____ de 20__.

_____

Carimbo e Assinatura do Gestor contratual

_____

Carimbo e Assinatura do Coordenador Geral responsável

(Documento datado e assinado eletronicamente)

GARCIAS GUEDES RODRIGUES JÚNIOR
Superintendente de Gestão de Pessoas - SGP/SEAD

JACYLENNE COELHO BEZERRA FORTES
Superintendente de Licitações e Contratos - SLC/SEAD

APROVO:

SAMUEL PONTES DO NASCIMENTO
Secretário de Estado da Administração do Piauí - SEAD/PI

Documento assinado eletronicamente por **GARCIAS GUEDES RODRIGUES JÚNIOR - Matr.0371160-9**, **Superintendente**, em 13/09/2023, às 11:43, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **9171075** e o código CRC **71F755B1**.

Referência: Processo nº 00002.007205/2023-09 SEI nº 9171075