EDITAL DE PREGÃO PRESENCIAL Nº 63/2022
REGISTRO DE PREÇOS Nº 14/2022

Processo Administrativo: 98/2022
Processo Eletrônico: e-50.809/2022
Tipo de Licitação: Menor Preço por Lote
Entrega dos envelopes: até às 10:30 horas (Horário de Brasília) do dia 07 de dezembro de 2022.
Data e horário de abertura: às 10:40 horas (Horário de Brasília) do dia 07 de dezembro de 2022.
Local: Sede administrativa da EMASA – 4ª Avenida, 250, Centro, Balneário Camboriú/SC.

O Diretor Geral da Empresa Municipal de Água e Saneamento de Balneário Camboriú - EMASA, entidade autárquica municipal, inscrita no CNPJ sob nº. 07.854.402/0001-00, face ao disposto no processo supra identificado, torna público que está instaurando licitação para **REGISTRO DE PREÇOS**, na modalidade **PREGÃO**, na forma **PRESENCIAL**, segundo as condições estabelecidas no presente Edital e seus Anexos, cujos termos igualmente o integram. **O critério de julgamento das propostas será o menor preço por Lote.** Este edital segue o que preceitua a legislação de regência, em especial a Lei n° 10.520, de 17 de julho de 2002; do Decreto Municipal n° 8.288, de 24 de agosto de 2016; do Decreto nº 6.973, de 9 de abril de 2013; e da Portaria nº 329/2016, 12 de maio de 2016, e ainda, no que couber, as determinações constantes da Lei n° 8.666, de 21 de junho de 1993; da Lei Complementar n° 123, de 14 de dezembro de 2006; da Lei Complementar nº 147, de 07 de agosto de 2014; do Decreto Federal nº 8.538, de 6 de outubro de 2015 e suas posteriores alterações.

1. DO OBJETO

1.1. A licitação tem como objeto o **REGISTRO DE PREÇOS PARA EVENTUAL CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO PARA PROTEÇÃO INTELIGENTE DE DADOS EM REPOUSO, ESTRUTURADOS E NÃO ESTRUTURADOS, CONTROLE DE ACESSO, VISIBILIDADE E RASTREABILIDADE DE UTILIZAÇÃO DE DADOS EM SERVIDORES DE ARQUIVSOS, BANCO DE DADOS LOCAIS E NUVEM, CUSTÓDIA DE**

CHAVES CRIPTOGRÁFICAS PARA AMBIENTES EM NUVEM (PÚBLICA, HÍBRIDA OU PRIVADA) COMPOSTA POR SOFTWARES E SERVIÇOS DE GARANTIA E SUPORTE TÉCNICO, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, SERVIÇOS DE TREINAMENTO, SERVIÇOS PARA INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS E SERVIÇOS ESPECIALIZADOS PARA ATENDER ÀS DEMANDAS DA EMASA, CONFORME ESPECIFICAÇÕES TÉCNICAS E DEMAIS CONDIÇÕES CONSTANTES NESTE EDITAL, conforme conveniência e necessidade estimada, para entrega e fornecimento ao longo de 12 (doze) meses, conforme descrição no Anexo I (Termo de Referência).

1.1.1. Os quantitativos e elementos suficientes para a compreensão do objeto da licitação, bem como, as condições para atendimento das obrigações necessárias ao cumprimento do objeto, encontram-se neste Edital e em seus Anexos.

1.2. Integram o presente Edital, para todos os fins e efeitos, os seguintes Anexos:

Anexo I – Termo de Referência
Anexo II – Minuta da Ata de Registro de Preços
Anexo III – Modelo de Credenciamento
Anexo IV – Modelo de Carta de Proposta de Preços
Anexo V – Modelo de Declaração Art. 7º da Constituição Federal
Anexo VI – Modelo de Declaração de Regularidade Fiscal
Anexo VII - Indicação de Preposto
Anexo VIII – Modelo de Enquadramento de Microempresa ou Empresa de Pequeno Porte.
Anexo IX – Declaração de Ausência de Parentesco.

1.3. A EMASA não se obriga a adquirir os itens relacionados dos licitantes vencedores, nem nas quantidades indicadas no Anexo I, podendo até realizar licitação específica para aquisição de um ou mais itens registrados, hipótese em que, em igualdade de condições, o beneficiário do registro terá preferência, nos termos do Art. 15, § 4º, da Lei nº 8.666/1993 e Art. 8º, § 1º, do Decreto nº 6.972/2013.

1.4. O preço máximo admitido pela EMASA no presente processo licitatório é **RESTRITO** e poderá ser informado após o encerramento da etapa de negociação.

2. DA SESSÃO PÚBLICA DO PREGÃO PRESENCIAL

2.1. A sessão pública deste Pregão Presencial será aberta por comando do Pregoeiro no endereço, data e horário discriminados no preâmbulo do edital.

2.2. Não havendo expediente na EMASA ou ocorrendo qualquer fato superveniente, que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e endereço eletrônico, salvo comunicação do Pregoeiro em sentido contrário.

3. DA DESPESA E DA DOTAÇÃO ORÇAMENTÁRIA

3.1 As despesas decorrentes da presente licitação correrão por conta da dotação orçamentária do exercício de 2022: funcional programática 35.001.17.512.1916, Projeto 2.189 – Manutenção das Atividades Administrativas da EMASA

3.2 O crédito necessário ao atendimento das despesas da presente licitação correrá à conta do Orçamento da Empresa Municipal de Água e Saneamento de Balneário Camboriú/SC.

4. DO CREDENCIAMENTO E PARTICIPAÇÃO

4.1. Poderão participar deste Pregão os interessados que atenderem todas as exigências deste Edital e seus Anexos.

4.2. No início da sessão, o representante da empresa licitante deverá apresentar os documentos necessários para a formulação de propostas e para a prática de todos os demais atos inerentes ao certame.

4.2.1 Caso a empresa se faça representar pelo seu proprietário, este deverá apresentar contrato social original ou cópia autenticada.

4.2.2 Caso seja designado outro representante, este deverá estar devidamente habilitado por meio de procuração, ou termo de credenciamento com carimbo e assinatura, podendo ser utilizado o modelo do Anexo II (modelo de credenciamento), acompanhado do contrato social, original ou cópia autenticada, da empresa representada.

4.3 O objeto social deverá ser compatível com o objeto da licitação.

4.4 No ato da sessão pública, o representante do licitante deverá identificar-se mediante a apresentação, ao Pregoeiro, de documento que comprove sua identidade, possibilitando a conferência dos dados com os informados nos documentos de credenciamento.

4.5 Cada credenciado poderá representar apenas um licitante. Na hipótese de tipo de licitação por item ou por lote, será admitido que um único credenciado represente mais de um licitante, desde que para itens ou lotes distintos.

4.6 Somente poderá participar da fase de lances verbais e demais atos relativos a este pregão o representante legal do licitante devidamente credenciado.

4.7 Só poderá se credenciar empresa que atenda ao item 4.3 deste edital de licitação.

4.8 **Não serão considerados os documentos de credenciamento inseridos nos envelopes de Proposta e/ou Habilitação.**

4.9 As Microempresas e Empresas de Pequeno Porte licitantes que queiram se valer dos benefícios da concedidos pela Lei Complementar nº 123/2006, deverão apresentar no **momento do Credenciamento**, um dos seguintes documentos:

a) Certidão Simplificada da Junta Comercial do Estado, da sede da licitante, com data de emissão não superior a 90 dias da data de abertura dos envelopes, para comprovação do seu enquadramento.

b) As sociedades simples, que não registram seus atos na Junta Comercial, deverão apresentar certidão do Registro Civil de Pessoas Jurídicas atestando seu enquadramento nas hipóteses do art. 3º da Lei Complementar nº 123/2006, cuja certidão deve estar atualizada, devendo ter sido emitida a menos de 120 (cento e vinte) dias da data marcada para a abertura da presente Licitação;

4.10 Junto a um dos dois documentos acima descritos a licitante deve apresentar, obrigatoriamente, declaração de enquadramento em conformidade com o art. 3º da Lei Complementar nº 123/2006, afirmando ainda que não se enquadram em nenhuma das hipóteses do § 4º do art. 3º da Lei Complementar nº 123/2006, conforme o modelo do presente Edital, Anexo VIII.

4.11 Ainda no credenciamento, os licitantes deverão apresentar declaração de que estão em situação regular perante as Fazendas Nacional, Estadual e Municipal, com a seguridade social (INSS e FGTS), bem como de que atendem às exigências do Edital quanto à habilitação jurídica, qualificação técnica e econômico-financeira, conforme o modelo do Anexo III (modelo de Declaração de Regularidade Fiscal). Esta declaração poderá ser preenchida no momento de sua apresentação através de formulário distribuído pelo Pregoeiro.

4.12 Os documentos para CREDENCIAMENTO e HABILITAÇÃO poderão ser apresentados em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas, pela junta comercial ou pela Comissão de Licitação, Pregoeiras ou Equipe de apoio de Pregão – mediante apresentação do original ou publicação na imprensa oficial.

4.12.1 Na hipótese de interessado pretender servir-se de autenticação por membro da Comissão, deverá oferecer previamente original e cópia, não se admitindo a autenticação depois de abertos os envelopes ou no momento da abertura.

4.12.2 A autenticação realizada pela Comissão de Licitação, Pregoeiras(os) ou Equipe de apoio de Pregão será realizada até o dia útil anterior ao da licitação.

4.13 Não poderá(ão) participar deste Pregão:

a) Fornecedor suspenso de participar de licitação e impedido de contratar com a EMASA, durante o prazo da sanção aplicada;

b) Fornecedor declarado inidôneo para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

c) Fornecedor impedido de licitar e contratar com o município, durante o prazo da sanção aplicada;

d) Fornecedor em processo de falência, recuperação judicial ou extrajudicial, sob concurso de credores, em dissolução, liquidação, fusão, cisão ou incorporação;

e) Sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum;

f) Sociedades estrangeiras não autorizadas a funcionar no país;

g) Consórcio de pessoas jurídicas, qualquer que seja sua forma de constituição.

5 DAS IMPUGNAÇÕES E ESCLARECIMENTOS

5.2 Até 02 (dois) dias úteis antes da data fixada para a abertura da Sessão Pública, qualquer pessoa poderá impugnar o ato convocatório do Pregão.

5.3 Caberá ao Pregoeiro decidir sobre a petição no prazo de até 24 (vinte e quatro) horas.

5.4 Acolhida a impugnação contra o ato convocatório, será designada nova data para a realização do certame.

5.5 A impugnação deve ser interposta por meio do Protocolo Eletrônico, disponível no site da EMASA, no qual a impugnante deverá:

5.5.1 No campo destinado ao assunto:

a) Selecionar a opção "PROTOCOLO DE RECURSOS OU IMPUGNAÇÕES A EDITAIS".

5.6 As impugnações também poderão ser protocoladas na sede administrativa da EMASA, em dias úteis, das 12h00 às 18h00 horas, sendo que não serão conhecidas as impugnações interpostas fora dos respectivos prazos legais.

5.7 Os pedidos de Esclarecimentos devem ser enviados ao Pregoeiro até 3 (três) dias úteis antes da data fixada para abertura da sessão pública, para o endereço eletrônico licitacao@emasa.com.br.

6. DA ENTREGA E DA ABERTURA DOS ENVELOPES

6.1. Até o dia e horário fixados para entrega dos envelopes no preâmbulo deste Edital, cada licitante deverá protocolar, na sede administrativa da EMASA, simultaneamente, sua proposta de preços e documentação de habilitação inseridas em 2 (dois) envelopes distintos, devidamente lacrados, indicando em suas partes externas e frontais as seguintes informações:

ENVELOPE Nº. 1 - "PROPOSTA DE PREÇOS"
EMPRESA MUNICIPAL DE ÁGUA E SANEAMENTO - EMASA
PREGÃO PRESENCIAL Nº 63/2022
REGISTRO DE PREÇOS Nº 14/2022
RAZÃO SOCIAL DO LICITANTE
CNPJ DO LICITANTE
ENDEREÇO COMPLETO
E-MAIL E TELEFONE

ENVELOPE Nº. 2 - "HABILITAÇÃO"
EMPRESA MUNICIPAL DE ÁGUA E SANEAMENTO - EMASA
PREGÃO PRESENCIAL Nº 63/2022
REGISTRO DE PREÇOS Nº 14/2022

RAZÃO SOCIAL DO LICITANTE
CNPJ DO LICITANTE
ENDEREÇO COMPLETO
E-MAIL E TELEFONE

6.2. Será aceita a remessa dos envelopes pelos Correios, desde que entregues na EMASA até a data e hora estipuladas para a entrega.

6.3. Neste caso, os envelopes e as declarações das quais dispõe o item deste edital deverão estar dentro de um terceiro envelope, postado para o seguinte endereço e identificação: Empresa Municipal de Água e Saneamento de Balneário Camboriú, Quarta Avenida, 250, Centro – Balneário Camboriú/SC, CEP – 88330-104; A/C Pregoeira – Pregão Presencial Nº. 10/2022 – Registro de Preços 01/2022. Contudo, a ausência de representante devidamente credenciado na sessão de abertura dos envelopes e julgamento, acarretará no impedimento do licitante participar da fase de lances e de exercer o direito de recurso.

6.4. Não poderão participar da licitação e nem serão consideradas licitantes as empresas que apresentarem envelopes após a data e horário definidos neste edital.

6.5. A reunião para recebimento e para abertura dos envelopes será pública, realizada em conformidade com este Edital e seus anexos, no local e horário já determinados, e cuja ata será dirigida por um Pregoeiro designado para este fim, a quem caberão o julgamento das propostas de preços e da habilitação, a classificação final, a adjudicação e o exame preliminar dos recursos.

7. DO PROCEDIMENTO E DO JULGAMENTO DAS PROPOSTAS

7.1 A reunião para recebimento e para abertura dos envelopes será pública, realizada em conformidade com este Edital e seus anexos, no local e horário já determinados, e será dirigida por um Pregoeiro designado para este fim, a quem caberão o julgamento das propostas de preços e da habilitação, a classificação final, a adjudicação e o exame preliminar dos recursos.

7.2 Após o credenciamento dos licitantes, o Pregoeiro abrirá os envelopes de proposta de preços e classificará o licitante com a proposta de menor preço, bem como aqueles com preços de até 10% (dez por cento) superiores àquele de menor preço para fazer lances verbais e sucessivos, até a proclamação do vencedor.

7.2.1 Nesta etapa serão desclassificadas as propostas que não atendam as exigências estabelecidas neste edital, porém sem verificação da aceitabilidade do preço.

7.3 Caso não sejam verificadas no mínimo 3 (três) propostas de preço nas condições definidas no subitem 7.2, serão classificadas as melhores propostas subsequentes, até o máximo de 3 (três), qualquer que seja o seu valor, para a apresentação de lances.

7.3.1 Os preços unitários máximos admitidos são os valores estimados pela EMASA, no orçamento em anexo ao processo licitatório.

7.4 Na sequência, terá início a etapa de apresentação de lances verbais, os quais deverão ser formulados de forma sucessiva, iniciando-se por aquele que tiver sido classificado com a maior proposta escrita. Os lances serão realizados de acordo com os quantitativos informados no objeto.

7.4.1 Caso duas ou mais propostas estejam com preços iguais, a ordem para a etapa de lances verbais será definido por sorteio.

7.4.2 Os lances deverão ter valores distintos e decrescentes em relação ao menor lance anteriormente apresentado.

7.4.3 O pregoeiro poderá estabelecer intervalo mínimo de diferença de valores entre os lances.

7.4.4 O valor que trata o item 7.4.3 poderá ser de até 5% do valor da menor proposta de preços apresentada no certame.

7.4.8 Aquele que renunciar a apresentação de lance na forma do subitem 7.4.2 ficará impedido de participar das próximas rodadas de lances verbais.

7.4.9 Encerrados os lances verbais pelo desinteresse dos licitantes, as ofertas serão ordenadas pelo critério de menor preço.

7.4.10 Não poderá haver desistência dos lances verbais ofertados, sujeitando-se o licitante desistente às penalidades constantes deste Edital.

7.4.11 Caso os licitantes não apresentem lances verbais, será verificada a conformidade entre a proposta escrita de menor preço e o valor estimado para a contratação, podendo o Pregoeiro negociar diretamente com o licitante para que seja obtido melhor preço.

7.5 Imediatamente após a etapa de lances, havendo a participação de microempresa ou empresa de pequeno porte com entrega do documento previsto no subitem 4.9 e 4.10, o Pregoeiro verificará a ocorrência de eventual empate, nos termos da Lei Complementar nº 123/06.

7.5.1 Considera-se empate a situação em que a proposta apresentada pela microempresa ou empresa de pequeno porte seja igual ou até 5% (cinco por cento) superior à proposta mais bem classificada não enquadrada como microempresa ou empresa de pequeno porte.

7.6 No caso de empate nos termos do subitem 7.5.1, será oportunizado à microempresa ou empresa de pequeno porte mais bem classificada apresentar proposta de preço inferior àquela considerada vencedora do certame no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, sob pena de preclusão, sendo que, exercida a oportunidade a que se refere este subitem, sua proposta será classificada em 1º lugar.

7.6.1 Verificando-se valores iguais nas propostas de microempresas e empresas de pequeno que estejam enquadradas na situação prevista no subitem 7.5.1, a primeira a apresentar oferta será decidida por sorteio a ser realizado pelo Pregoeiro.

7.6.2 Caso a microempresa ou empresa de pequeno porte recuse o benefício previsto no subitem 9.6 serão convocadas as remanescentes que porventura se enquadrem na hipótese do subitem 9.5.1, na ordem classificatória, para o exercício do mesmo direito.

7.6.3 Não verificada a hipótese prevista no subitem 7.5 ou não exercido o direito previsto no subitem 7.6, será classificada em 1º lugar a proposta originalmente vencedora do certame.

7.7 Findos os lances verbais e ordenados os licitantes pelo critério do menor preço, o Pregoeiro examinará a aceitabilidade do valor apresentado, decidindo motivadamente a respeito.

7.7.1 Nesta etapa, é facultado ao Pregoeiro negociar o preço ofertado diretamente com o representante, visando a sua redução para compatibilização com o orçamento estimativo da EMASA.

7.7.2 Confirmada a efetividade do lance ou proposta que obteve a primeira colocação na etapa de julgamento, ou que passe a ocupar esta posição em decorrência da desclassificação de outra que tenha obtido colocação superior, o Pregoeiro deverá negociar condições mais vantajosas com quem o apresentou.

7.7.2.1 A negociação deverá ser feita com os demais licitantes, segundo a ordem inicialmente estabelecida, quando o preço do primeiro colocado, mesmo após a negociação, permanecer acima do orçamento estimado.

7.7.2.2 Se depois de adotada a providência referida no item 7.7.2.1 não for obtido valor igual ou inferior ao orçamento estimado para a contratação, será revogada a licitação.

7.8 Havendo aceitação do menor preço, será efetuada a abertura do envelope de habilitação dos licitantes classificados nesta condição para verificação da documentação apresentada e sua conformidade com as exigências do edital.

7.9 Serão inabilitados os licitantes cuja documentação não atender às exigências deste edital.

7.10 Caso não seja aceita a proposta vencedora ou se o licitante não atender as exigências do edital, o Pregoeiro examinará as ofertas subseqüentes, na ordem de classificação, até a apuração de uma proposta que atenda a todas as exigências, sem prejuízo do disposto no subitem 7.7.1.

7.11 Ultrapassada a fase de habilitação, será(ão) declarados(s) o(s) vencedor(es) do certame.

7.11.1 No caso de necessidade de apresentação de planilha de composição dos preços, o Pregoeiro poderá fixar o prazo de até 2 (dois) dias úteis (a contar do encerramento da sessão em que ocorrer a declaração do licitante vencedor), para a Licitante detentora da melhor oferta encaminhar nova Proposta de Preços (que não poderá cotar preço unitário e global superior ao orçamento estimativo da EMASA) dentre outros documentos exigidos no Edital, devidamente ajustados ao valor ofertado e registrado como de menor lance.

7.12 Após o julgamento definitivo das propostas de preços, de eventuais recursos e classificação final, o Pregoeiro encaminhará o processo licitatório para adjudicação do objeto ao(s) vencedor(es) e homologação pela autoridade competente.

7.13 Poderá o Pregoeiro, caso julgue conveniente, suspender os trabalhos durante a sessão de abertura dos envelopes e julgamento, devendo neste caso, informar a data e o horário de reabertura.

7.14 No caso do adjudicatário decair do direito de executar o objeto licitado, a EMASA poderá revogar esta licitação, ou convocar os licitantes remanescentes, na ordem de classificação, para contratar, em igual prazo e nas mesmas condições propostas pelo primeiro classificado.

7.15 Da sessão de abertura dos envelopes e julgamento lavrar-se-á ata circunstanciada, na qual serão registradas as ocorrências. A ata deverá ser assinada pelo Pregoeiro e pelos representantes dos licitantes presentes.

7.16 Os envelopes de habilitação dos licitantes cujas propostas foram classificadas ficarão de posse do Pregoeiro até o adimplemento das obrigações contratuais, quando serão inutilizados.

8. DA ACEITABILIDADE DAS PROPOSTAS

8.1. Encerrada a etapa competitiva, o Pregoeiro, **auxiliado pela equipe de apoio**, examinará as propostas classificadas em primeiro lugar quanto à compatibilidade com as especificações técnicas do objeto descritas no Anexo I (Termo de Referência) e ao preço ofertado.

8.2. **O critério de julgamento das propostas será o menor preço, nos termos do Termo de Referência do Edital.**

8.3. Não se aceitará proposta com valores unitário ou global manifestamente inexequíveis, ressalvado o disposto nos itens seguintes.

8.4. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a serviços/produtos/materiais e instalações de propriedade do licitante, para os quais ele renuncie à parcela ou à totalidade de remuneração.

8.4.1. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.5. Havendo necessidade, o Pregoeiro suspenderá temporariamente o Pregão para que seja analisada a compatibilidade dos produtos/materiais ofertados com as características constantes do presente Edital, podendo, **a critério da equipe técnica do Pregão**, serem solicitadas amostras ou documentação com informações técnicas dos produtos/materiais nos termos deste Edital.

8.5.1. Ocorrendo a suspensão prevista no **item 8.5**, o Pregoeiro notificará os participantes da data e horário de reabertura do Pregão para conclusão da etapa de aceitação das propostas e consequente início das demais etapas do certame.

8.6. A desclassificação de uma proposta por incompatibilidade do produto/material ofertado com as especificações descritas no Termo de Referência **poderá, conforme caso e a juízo do Pregoeiro, ser precedida de pareceres técnicos da equipe de apoio do Pregão**, ou de técnicos pertencentes ao quadro de pessoal da EMASA ou, ainda, de pessoas físicas ou jurídicas estranhas a ela.

8.7. Se a proposta que apresentou o menor lance não for aceitável ou se o licitante não atender às exigências de habilitação contidas neste Edital, o Pregoeiro examinará a proposta subseqüente, e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às exigências do Edital.

8.8. O Pregoeiro poderá encaminhar contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida uma melhor proposta, observando os critérios de julgamento, não sendo admitido negociar condições diferentes das previstas neste Edital.

9. DA APRESENTAÇÃO DA AMOSTRA E PROVA DE CONCEITO

9.1. A licitante vencedora da etapa de lances e legalmente habilitada será submetida à prova de conceito a fim de comprovação de atendimento às exigências técnicas e demais requisitos obrigatórios, contidos no Anexo I deste Edital.

9.2. A prova de conceito será realizada em sessão aberta a iniciar mediante solicitação do pregoeiro, começando no primeiro dia útil subsequente, caso este prazo coincida com feriado ou final de semana, no horário de 08h às 12h e das 14h às 18h.

9.3. A solução apresentada que não atender a 100% (cem por cento) das exigências do caderno de testes Anexo I, da prova de conceito, será considerada inapta, estando, portanto, desclassificada a licitante vencedora, sendo convocada a licitante seguinte na ordem classificatória para realização de prova de conceito e assim sucessivamente até que uma das licitantes participantes apresente solução que atenda plenamente às exigências deste documento.

9.4. A licitante declarada vencedora na etapa de lances que não comparecer para efetuar a prova de conceito, se recusar por qualquer motivo a efetuar a prova de conceito e/ou não atender aos critérios estabelecidos neste Edital, inclusive quanto aos requisitos mínimos considerados, será imediatamente considerada inapta para assinatura do contrato, sendo imediatamente desclassificada.

9.5. Serão avaliados todos os itens constantes do roteiro do Anexo I, integrante deste Edital, respeitado o atendimento de todas as características descritas em cada funcionalidade.

9.6. A realização da prova de conceito e a verificação do cumprimento dos requisitos técnicos obrigatórios previstos no Termo de Referência ficarão a cargo da Comissão Técnica, integrada por empregados designados pela EMASA.

9.7. A prova será executada e julgada pelos membros da Comissão Técnica do CONTRATANTE, com base nos itens constantes Prova de Conceito, Anexo I.

9.8. A comprovação do atendimento às características técnicas especificadas no Termo de Referência dar-se-á por meio da documentação da solução e os datasheet.

9.9. A comprovação das exigências para todos os itens deverá ser realizada em até 05 (cinco) dias úteis, caso necessite deste prazo para conclusão de demonstração.

9.10. Os testes poderão ser executados nas dependências da EMASA obedecendo aos seguintes critérios:

9.10.1. Toda a infraestrutura necessária à execução da Prova de Conceito deverá ser fornecida pela Licitante, sendo a EMASA responsável apenas pelo fornecimento do espaço físico adequado e energia elétrica.

9.11. A prova de conceito constituirá da realização do checklist das características/funções mínimas obrigatórias, conforme Prova de Conceito, Anexo I.

9.12. Opcionalmente, serão aceitos testes realizados em ambiente de Nuvem.

9.13. Para a análise do software/solução e da prova de conceito, a sessão será suspensa e retomada somente após a análise acerca da aceitação do software/solução a que se refere, exarando-se a decisão em documento expedido pelo Pregoeiro posteriormente. O acompanhamento da análise de conceito é facultado aos demais licitantes interessados.

9.14. Se, ao final da execução da Prova de Conceito, ficar comprovado o cumprimento de todos os requisitos, a Comissão Técnica emitirá Termo de Verificação, com vistas à aceitação da proposta da Licitante.

10. DA PROPOSTA DE PREÇOS

10.1. O licitante deverá encaminhar proposta exclusivamente na forma indicada no item 6 deste edital.

10.2. As propostas deverão ser datilografadas ou digitadas em uma via, preferencialmente em papel timbrado do licitante, sem entrelinhas, emendas, rasuras ou borrões que afetem sua idoneidade, assinadas e rubricadas em todas as folhas pelo representante legal, contendo as seguintes informações:

a) razão social e nº do CNPJ do proponente, a modalidade e o número desta licitação, nome do responsável pela proposta, endereço, telefone, fax e e-mail, se houver;

b) especificação do objeto cotado;

c) o valor unitário e total, de acordo com os quantitativos do objeto, em reais (R$), com duas casas decimais, incluindo todos os tributos, encargos sociais e trabalhistas, fretes e quaisquer outras despesas que incidam direta ou indiretamente sobre o objeto desta licitação;

d) o prazo para execução do objeto não superior ao previsto no Termo de Referência (Anexo I) deste Edital;

e) prazo de pagamento de até 30 (trinta) dias após a entrega das soluções/softwares, mediante apresentação de nota fiscal com toda documentação completa exigida e aprovação da Comissão de Recebimento de Bens, Materiais e Serviços da EMASA;

f) o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias, a contar da entrega dos envelopes.

10.3. Na omissão dos prazos de fornecimento, pagamento e validade da proposta, serão considerados os constantes do edital e na divergência entre o preço unitário e total, prevalecerá o preço unitário.

10.4. Preferencialmente, para facilitar o julgamento por parte do pregoeiro, solicita-se aos licitantes que apresentem suas propostas nos moldes do Anexo IV (modelo de proposta de preços).

10.5. As propostas serão irretratáveis e irrenunciáveis, na forma da lei.

10.6. Cada licitante poderá apresentar apenas uma proposta de preços.

10.7. As propostas comerciais deverão conter obrigatoriamente, **sob pena de desclassificação**:

a) **O preço unitário e total do item cotado**, com formulado em moeda nacional, considerando-se somente 2 (duas) casas decimais, devendo estar incluídos todos os custos com frete, tributos, seguros, e quaisquer outras despesas que incidam ou venham a incidir sobre o objeto desta licitação.

b) **A descrição do produto/material cotado**.

10.8. O Cadastro Nacional da Pessoa Jurídica - CNPJ da empresa proponente deverá ser o mesmo da que efetivamente fornecerá os produtos/materiais objetos da presente licitação.

10.9. **O prazo de validade das propostas comerciais será de 60 (sessenta) dias**, contados da data de abertura da sessão pública estabelecida neste Edital, salvo o disposto no **item 13.6** do presente Edital.

10.9.1. Decorrido o prazo de validade das propostas sem convocação para assinatura da Ata de Registro de Preços, ficam os licitantes liberados dos compromissos assumidos.

11. DA HABILITAÇÃO

11.1. Para fins de habilitação, os licitantes deverão apresentar os seguintes documentos:

a) Registro Comercial, no caso de empresa individual;

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, no caso de sociedades comerciais e, no caso de sociedades por ações, acompanhado dos documentos comprobatórios de eleição de seus administradores (os licitantes que atenderem ao item 4.1.2 e apresentarem o ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, no momento do credenciamento, estão dispensados de apresentá-lo novamente no envelope de habilitação);

c) Decreto de autorização, no caso de empresa ou sociedade estrangeira em funcionamento no país e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

d) Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

e) Comprovante de regularidade fiscal perante a Fazenda Federal, referente a débitos relativos a tributos federais e à dívida ativa da União;

f) Comprovante de regularidade fiscal perante a Fazenda Estadual do domicílio ou sede do licitante;

g) Comprovante de regularidade fiscal perante a Fazenda Municipal do domicílio ou sede do licitante;

h) Certidão negativa de Falência ou Recuperação Judicial, expedida pelo distribuidor da sede da pessoa jurídica, com data de emissão não superior a 180 (cento e oitenta) dias, quando não constar expressamente no documento o seu prazo de validade.

OBS: Considerando a implantação do sistema eproc no Poder Judiciário de Santa Catarina, a partir de 1º/4/2019, as certidões dos modelos "Cível" e "Falência, Concordata e Recuperação Judicial" deverão ser solicitadas tanto no sistema eproc quando no SAJ. As duas certidões deverão ser apresentadas conjuntamente, caso contrário não terão validade.

i) Comprovante de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS);

j) Certidão Negativa de Débitos Trabalhistas a ser emitida pela Justiça do Trabalho (CNDT);

k) Declaração de que a empresa não emprega menores de 18 anos em trabalho noturno, perigoso ou insalubre, nem menores de 16 anos de idade, salvo na condição de aprendiz, a partir de 14 anos, conforme disposto no inciso XXXIII, do art. 7º da Constituição Federal, emitida pelo próprio licitante conforme modelo Anexo V.

l) Declaração de Ausência de Parentesco, conforme modelo Anexo IX.

m) Indicação de Preposto, conforme modelo Anexo VII.

n) Atestado(s) de Capacidade Técnica ou Declaração(s) emitida(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante realizou fornecimento compatível em característica, com o objeto da presente licitação, atestando, inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais, no(s) atestado(s) deverão estar contemplados, no mínimo, as seguintes parcelas de maior relevância e valor significativo:

n.1) Fornecimento/licenciamento de Solução de Gerenciamento e Segurança da Informação para proteção de dados em repouso e em trânsito, controle de acesso, visibilidade e rastreabilidade de utilização em servidores de arquivo, banco de dados, utilizando custódia de chaves criptográficas composta por software e hardware.

n.2) Fornecimento/licenciamento de software/solução de Gerenciamento de Segurança da informação (segurança digital), contemplando ferramenta de Criptografia e serviço de instalação configuração, capacitação e integração.

n.3) O(s) atestado(s) deverá(ão) conter o nome das empresas declarantes, a identificação do nome e a assinatura do responsável, bem como o número de telefone para contato.

n.4) O (s) atestado(s) deverá(ão) estar acompanhados de cópias dos respectivos contratos/Notas Fiscais, bem como demais documentos comprobatórios do efetivo fornecimento.

Os atestados ou declarações deverão ser emitidos em papel timbrado da emitente, datado e assinado e, deverá se referir a fornecimentos concluídos, com especificações

dos fornecimentos realizados, e informações relativas ao desempenho do fornecimento.

o) Para efeito de qualificação técnico profissional, a licitante deverá apresentar documento que ateste possuir pelo menos 1 (um) profissional com certificação CISSP (Certified Information Systems Security Professional) ou CISM (Certified Information Security Manager), concedida pela ISC2 (International Info System Security Certification Consortium) ou concedida pelos representantes e/ou parcerias oficiais da ISC2 no Brasil ou no exterior. O profissional acima indicado deverá integrar quadro técnico da empresa, na data de apresentação da proposta, comprovado por meio das seguintes formas abaixo indicadas:

o.1) mediante contrato social (no caso de sócio); ou

o.2) registro na carteira profissional, ficha de empregado ou contrato de trabalho; ou

o.3) contrato de prestação de serviços, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços quando da assinatura do contrato entre a Licitante e a EMASA.

p) Catálogo, folder, prospectos, fotos ou folhetos ilustrativos, ou manual técnico elaborado pela fabricante, ou documento extraído de consulta realizada pela internet, devendo, nesse caso, ser indicado o endereço eletrônico, que possibilite uma análise clara e inequívoca sobre as características do objeto ofertado.

11.2. A validade das certidões exigidas corresponderá ao prazo fixado nos próprios documentos. Caso as mesmas não contenham expressamente o prazo de validade, a EMASA convenciona o prazo como sendo de 60 (sessenta) dias, a contar da data de sua expedição, ressalvada a hipótese de o licitante comprovar que o documento tem prazo de validade superior ao convencionado, mediante juntada de norma legal pertinente.

11.3. O Pregoeiro verificará, ainda, **sob pena de inabilitação**:

a) A existência de registros impeditivos da contratação no Cadastro Nacional de Empresas Inidôneas e Suspensas/CGU, disponível no Portal da Transparência (http://www.portaltransparencia.gov.br), além da habitual pesquisa já realizada no módulo SICAF do sistema SIASG (consulta pelo CNPJ), em atenção ao art. 97, caput e parágrafo único, da Lei n.º 8.666/1993;

b) A composição societária das empresas a serem contratadas no sistema SICAF, a fim de se certificarem se entre os sócios há servidores do próprio órgão contratante - EMASA, abstendo-se de celebrar contrato nessas condições, em atenção ao art. 9º, inciso III, da Lei nº 8.666/1993;

c) O CNIA (cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa) – Cadastro Nacional Conselho Nacional de Justiça, acesso pelo site (http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php), consulta pelo CNPJ;

d) Lista de declarados irregulares, inidôneos e inabilitados pelo Tribunal de Contas da União disponível no site (http://portal.tcu.gov.br/responsabilizacao-publica/licitantes-inidoneas/).

11.3.1. **Sendo constatado qualquer impedimento de licitar ou contratar por parte do licitante em qualquer das consultas anteriores, o mesmo será inabilitado.**

11.4. O Pregoeiro poderá consultar sítios oficiais de órgãos e entidades emissoras de certidões para verificar as condições de habilitação dos licitantes.

11.5. Os documentos encaminhados deverão estar em nome do licitante, com indicação do número de inscrição no CNPJ.

11.6. Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz.

11.7. Os documentos de habilitação relacionados acima deverão estar válidos e em vigor na data de sessão de abertura dos envelopes e julgamento.

11.8. Os documentos para habilitação poderão ser apresentados em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas pela junta comercial ou membro da Comissão de Registro de Preço – mediante apresentação do original ou publicação na imprensa oficial.

11.8.1. Na hipótese de interessado pretender servir-se de autenticação por membro da Comissão, deverá oferecer previamente original e cópia, não se admitindo a autenticação depois de abertos os envelopes ou no momento da abertura.

11.8.2. Para esse procedimento a comissão ficará a disposição dos interessados no horário de expediente da EMASA, na sede Administrativa da Autarquia.

11.9. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para língua portuguesa, efetuada por tradutor juramentado, e também devidamente consularizados ou registrados no cartório de títulos e documentos. Os documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados em cartório de títulos e documentos.

11.10. Os documentos remetidos pelos licitantes na forma do *caput* poderão ser solicitados em original ou por cópia autenticada a qualquer momento, em prazo a ser estabelecido pelo Pregoeiro.

11.11. Se o licitante não atender às exigências de habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este Edital.

11.12. Constatado o atendimento às exigências fixadas neste Edital, o licitante será declarado vencedor.

12. DA SUBCONTRATAÇÃO

12.1. Será admitida a subcontratação do item de **Serviço de Treinamento Oficial**, sendo uma parcela a qual exige-se uma qualificação quanto a formação do objeto. Este limite deverá compreender os limites mínimo e máximo de 5% e 10%, respectivamente, do valor total do contrato, nas seguintes condições:

12.1.1. É vedada a sub-rogação completa ou da parcela principal da obrigação. São obrigações adicionais da contratada, em razão da subcontratação;

12.1.2. Apresentar a documentação de regularidade fiscal das microempresas e empresas de pequeno porte subcontratadas, sob pena de rescisão, aplicando-se o prazo para regularização previsto no § 1º do art. 4º do Decreto nº 8.538, de 2015;

12.1.3. 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;

12.1.4. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, bem como pela padronização, pela compatibilidade, pelo gerenciamento centralizado e pela qualidade da subcontratação, 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. Não será aplicável a exigência de subcontratação quando a licitante for qualificada como microempresa ou empresa de pequeno porte.

13. DOS RECURSOS ADMINISTRATIVOS

13.1. Após declarado o(s) vencedor(es), qualquer licitante poderá, sob pena de preclusão, manifestar imediata, formal e motivadamente sua intenção de recorrer, quando será aberto o prazo de 3 (três) dias para apresentação das razões do recurso, ficando desde logo, os demais licitantes intimados para prestar as contrarrazões em igual prazo, que começara a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

13.1.1. A intenção de recurso meramente protelatória, sem plausibilidade, poderá ser rechaçada pelo Pregoeiro, motivando as razões na própria Ata.

13.1.2. Os recursos interpostos contra decisão do Pregoeiro não terão efeito suspensivo.

13.2. As razões e contrarrazões dos recursos deverão ser dirigidas ao Diretor Geral da Empresa Municipal de Água e Saneamento de Balneário Camboriú.

13.3. **O recurso deverá ser interposto por meio do Protocolo Eletrônico, disponível no site da EMASA, no qual a recorrente deverá:**

13.3.1. **No campo destinado ao assunto:**

a) **Selecionar a opção "PROTOCOLO DE RECURSOS OU IMPUGNAÇÕES A EDITAIS".**

13.4. Os recursos também poderão ser protocolados na sede administrativa da EMASA, situada na Quarta Avenida, nº. 250, em Balneário Camboriú, nos dias úteis em horário compreendido entre as 12:00 e 18:00 horas.

13.5. Recebido o recurso, o Pregoeiro poderá reconsiderar sua decisão ou remeter o processo devidamente informado para a autoridade superior para deliberação.

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. Decididos os recursos eventualmente interpostos, o processo licitatório será submetido ao Diretor Geral da EMASA, para que se proceda à devida homologação e conseqüente adjudicação do objeto licitado ao licitante vencedor.

15. DA ATA DE REGISTRO DE PREÇOS

15.1. Após a homologação do Pregão, o registro de preços observará, entre outras, as seguintes condições:

a) Serão registrados na Ata de Registro de Preços os preços e quantitativos do licitante mais bem classificado durante a etapa competitiva.

b) O preço registrado com indicação dos fornecedores será divulgado no site da EMASA e ficará disponibilizado durante a vigência da Ata de Registro de Preços.

15.2. Homologado o Pregão, a EMASA convocará o licitante vencedor, por meio de endereço eletrônico constante na proposta de preços e via publicação no site da EMASA para, **no prazo de 5 (cinco) dias úteis a partir do recebimento da convocação**, assinar a Ata de Registro de Preços e/ou retirar ou confirmar o recebimento da nota de empenho.

15.2.1. **Cabe ao licitante vencedor verificar o site da EMASA e sua caixa de e-mails para verificar sua convocação para assinar a ATA DE REGISTRO.**

15.2.2. **Será obrigatória assinatura eletrônica da ata/contrato, mediante uso da certificação digital, caso o representante legal da licitante não a possua, o prazo para regularização será o mesmo do item 14.2.**

15.3. O não comparecimento do licitante vencedor, dentro do prazo de 5 (cinco) dias úteis, após regularmente convocado para a assinatura da Ata de Registro de Preços e/ou para confirmar o recebimento da nota de empenho, ensejará a aplicação de multa de 10% (dez por cento) sobre o valor total da Ata de Registro de Preços.

15.4. O prazo mencionado acima poderá ser prorrogado uma só vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração, conforme previsto no § 1º, do art. 64, da Lei nº 8.666/93.

15.5. Caso o licitante classificado em primeiro lugar não assine a Ata de Registro de Preços, não apresente situação regular no ato da assinatura ou não retire ou confirme o recebimento da

nota de empenho serão examinadas as ofertas subsequentes, bem como os respectivos documentos de habilitação dos proponentes, convocando-os, na ordem de classificação, para assinar a Ata de Registro de Preços, mantido o preço do primeiro classificado na licitação ou proposta ainda mais favorável para a Administração.

15.6. No ato da assinatura da Ata de Registro de Preços e durante a vigência da mesma, o licitante vencedor deverá manter as mesmas condições para habilitação e classificação da proposta.

15.7. Publicada na Imprensa Oficial, a Ata de Registro de Preços terá efeito de compromisso de fornecimento, nas condições estabelecidas neste Edital, conforme disposto na legislação pertinente.

15.8. **O prazo de validade da Ata de Registro de Preços será de 12 (doze) meses.**

15.9. A futura contratação dos fornecedores com preços registrados será formalizada pela EMASA por intermédio da emissão de Nota de Empenho.

15.10. As supressões de saldo de quantitativos a adquirir, ainda não contemplados nos pedidos de fornecimento, poderão atingir o limite de 100% (cem por cento).

15.11. A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, facultando-se a realização de licitação específica para a aquisição pretendida, sendo assegurado ao fornecedor beneficiário do registro preferência de fornecimento em igualdade de condições.

15.12. A associação do licitante vencedor com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação devem ser comunicadas à EMASA para que esta delibere sobre a adjudicação do objeto ou manutenção do contrato, sendo essencial, para tanto, que a nova empresa comprove atender a todas as exigências de habilitação previstas no Edital.

15.13. Durante a vigência da Ata, os preços registrados serão fixos e irreajustáveis, exceto nas hipóteses previstas no art. 10 do Decreto nº 6.972/13, observadas, em qualquer caso, as disposições contidas na alínea "d'" do inciso II do *caput* do art. 65 da Lei nº 8.666/93.

15.13.1. Nessa hipótese, a Administração, se julgar conveniente, poderá optar por cancelar a Ata e iniciar outro processo licitatório.

15.14. A EMASA realizará periodicamente pesquisa de mercado para comprovação da vantajosidade.

15.15. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, a EMASA convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.

a) O fornecedor que não aceitar reduzir seus preços aos valores praticados pelo mercado será liberado do compromisso assumido, sem aplicação de penalidade.

b) A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

15.16. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, a EMASA poderá:

a) liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

b) convocar os demais fornecedores para assegurar igual oportunidade de negociação.

15.16.1. Não havendo êxito nas negociações, a EMASA deverá proceder à revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

15.17. O registro de preços será cancelado, por meio de processo administrativo específico e assegurados o contraditório e a ampla defesa, quando houver razões de interesse público, devidamente motivadas e justificadas ou quando o fornecedor:

a) Não cumprir as condições da Ata de Registro de Preços;

b) Não retirar a respectiva Nota de Empenho no prazo estabelecido pelo Departamento de Contratos e Licitações da EMASA, sem justificativa aceitável;

c) Deixar de cumprir qualquer condição de habilitação exigida no processo licitatório;

d) Não aceitar reduzir o preço registrado, na hipótese de este se tornar superior aos praticados no mercado;

e) Sofrer sanção prevista nos incisos III ou IV do *caput* do art. 87 da Lei nº 8.666/93, ou no art. 7º da Lei nº 10.520/02.

15.17.1. O cancelamento de registros nas hipóteses previstas nas **alíneas "a"**, **"b"**, **"d"** e **"e"** será formalizado por despacho da EMASA, assegurado o contraditório e a ampla defesa.

15.18. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da Ata, devidamente comprovados e justificados:

a) por razão de interesse público; ou

b) a pedido do fornecedor.

15.19. O fornecedor poderá solicitar o cancelamento do seu registro de preço na ocorrência de fato superveniente que venha a comprometer a perfeita execução contratual, decorrentes de casos fortuitos ou de força maior, devidamente comprovados.

15.20. Durante a validade da Ata de Registro de Preços, o fornecedor não poderá alegar a indisponibilidade do produto/material ofertado, sob pena de lhe serem aplicadas as sanções previstas neste Edital e na Lei.

15.21. Caberá à EMASA a prática de todos os atos de controle e administração do registro de preços decorrentes desta licitação, na forma do art. 2º do Decreto nº 6.972/13 e demais normas pertinentes.

16. DAS CONDIÇÕES DE FORNECIMENTO

16.1. As quantidades indicadas no Termo de Referência referem-se à previsão de consumo total no período de vigência da Ata, ficando as entregas condicionadas à emissão da nota de empenho pela EMASA.

16.1.1. O encaminhamento da nota de empenho será efetuado mediante envio, pelo Departamento responsável da EMASA, de correspondência eletrônica ao endereço eletrônico da contratada constante na proposta de preços.

16.2. No ato de entrega do objeto, a contratada deve apresentar documento fiscal válido correspondente ao fornecimento.

16.3. **Os produtos/materiais deverão ser entregues no prazo e locais indicados no Termo de Referência.**

16.4. Os produtos/materiais serão recebidos provisoriamente no ato da entrega, para efeito de posterior verificação da conformidade do item com as especificações constantes do Anexo I e na proposta comercial.

16.5. Os produtos/materiais poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste edital e/ou na proposta comercial, devendo ser substituídos às expensas do fornecedor no prazo de 10 (dez) dias, contado a partir da data da notificação.

16.5.1. Neste caso serão interrompidos os prazos de recebimento e suspenso o pagamento, até que sanada a situação, quando ocorrerá um novo recebimento provisório, e o reinício de contagem dos prazos.

16.5.2. Os produtos/materiais rejeitados deverão ser retirados no endereço informado no Anexo I, às custas do fornecedor.

16.5.3. A EMASA não arcará com nenhum ônus advindo da troca de itens rejeitados, nem mesmo enviará produtos/materiais via correio ou por qualquer outra forma.

16.6. Os produtos/materiais serão recebidos definitivamente no prazo de 5 (cinco) dias, contado a partir da data da entrega, após a verificação da qualidade e quantidade do material e consequente aceitação, na forma do art. 73, inciso II e parágrafos, da Lei nº 8.666/93, mediante a lavratura de termo circunstanciado.

16.7. Na hipótese de o termo circunstanciado ou a verificação não serem, respectivamente, lavrado ou procedida dentro dos prazos fixados, reputar-se-ão como realizados, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

16.8. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade do fornecedor por quaisquer danos causados à Administração ou a terceiros, decorrentes da utilização do material fornecido.

16.9. O fornecedor deverá informar, se for o caso, qualquer condição especial para armazenamento e/ou transporte do produto/material fornecido.

17. DAS CONDIÇÕES DE PAGAMENTO

17.1. O pagamento será efetuado mensalmente e em até 30 (trinta) dias, mediante apresentação de medição, quando for o caso, e da nota fiscal devidamente aprovada pela respectiva Comissão de Recebimento da EMASA, nas condições da proposta apresentada.

17.2. **A NF só poderá ser emitida após aprovação da medição e liberação da autorização para emissão da NF pelo fiscalizador do contrato da EMASA.**

17.3. Todos os pagamentos serão realizados exclusivamente por depósito bancário.

17.4. **É CONDIÇÃO INDISPENSÁVEL PARA A EFETUAÇÃO DO PAGAMENTO, A COMPROVAÇÃO, POR PARTE DO CONTRATADO, DA REGULARIDADE COM O INSS E FGTS.**

17.5. **AS NOTAS FISCAIS DEVERÃO INDICAR O Nº DE SUA NOTA DE EMPENHO E, QUANDO FOR O CASO, O NÚMERO DO CONTRATO.**

17.6. **O NÃO CUMPRIMENTO DOS ITENS 16.4 E 16.5 CULMINAM NA DEVOLUÇÃO DA NOTA FISCAL.**

17.7. Se o contratante não efetuar o pagamento no prazo previsto e tendo o contratado, à época, adimplido integralmente as obrigações avençadas, inclusive o disposto no subitem 14.2, os valores devidos serão monetariamente atualizados, a partir do dia de seu vencimento e até o dia de sua liquidação, segundo os mesmos critérios adotados para atualização de obrigações tributárias, conforme estabelecido no artigo 117 da Constituição Estadual.

18. DA FISCALIZAÇÃO E ACOMPANHAMENTO

18.1. Para o acompanhamento, controle, fiscalização e avaliação do objeto será indicado um servidor responsável, designado pelo gestor da unidade, podendo ser auxiliado por outro servidor igualmente designado.

18.2. A fiscalização será exercida no interesse da Administração, não excluindo nem reduzindo a responsabilidade da contratada, inclusive perante terceiros, por qualquer irregularidade e, na sua ocorrência, não implicará a corresponsabilidade do Poder Público, de seus agentes ou prepostos.

18.3. Quaisquer exigências da fiscalização, dentro do objeto da licitação, deverão ser prontamente atendidas pela contratada, sem ônus para a EMASA.

18.4. A fiscalização deste contrato será realizada pela COMISSÃO DE RECEBIMENTO DE BENS E SERVIÇO, e-mail comissao.materiais@emasa.com.br, telefone (47) 3261 0000.

18.5. O(s) fiscal(ais) anotará(ão) em registro próprio, todas as ocorrências relacionadas com a execução dos serviços contratados, determinando o que for necessário à regularização das faltas ou defeitos observados.

18.6. A omissão, total ou parcial, da fiscalização não eximirá o fornecedor da integral responsabilidade pelos encargos ou serviços que são de sua competência.

18.7. Ao tomarem conhecimento de qualquer irregularidade ou inadimplência por parte da contratada, os titulares da fiscalização deverão, de imediato, comunicar por escrito ao órgão de administração do contratante, que tomará as providências para que se apliquem as sanções previstas na lei, no Edital e neste Termo de Referência, sob pena de responsabilidade solidária pelos danos causados por sua omissão.

19. DAS SANÇÕES ADMINISTRATIVAS

19.1. O licitante/fornecedor que, convocado dentro do prazo de validade de sua proposta, não assinar a Ata de Registro de Preços, deixar de entregar documentação exigida neste Edital, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta/lance, falhar ou fraudar na execução da Ata/Contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedido de licitar e de contratar com a EMASA e o Município, pelo prazo de até 2 (dois) anos, sem prejuízo das sanções previstas neste Edital e na Ata de Registro de Preços e das demais cominações legais.

19.1.1. O encaminhamento de Ofício de Notificação poderá ser efetuado pelo Departamento responsável da EMASA por meio de endereço eletrônico, para fins de garantia do direito à ampla defesa em caso de inexecução total ou parcial de quaisquer dos atos dispostos no item precedente.

19.1.2. Além do envio do email, a EMASA publicará em jornal de circulação local o extrato do Ofício de Notificação.

19.1.3. É de responsabilidade do Contratado verificar sua caixa de entrada de emails e as publicações oficiais da EMASA.

19.2. Se no decorrer da sessão pública da licitação ou na execução do objeto do presente Edital ficar comprovada a existência de qualquer irregularidade ou ocorrer inadimplemento contratual pelo qual possa ser responsabilizado o licitante/contratado, este poderá sofrer as seguintes penalidades:

a) Advertência por escrito;

b) Multa de 10% (dez por cento), calculada sobre o valor total atualizado da proposta ou lance, na hipótese de desistência injustificada da proposta ou lance após a fase de habilitação;

c) Multa de 10% (dez por cento), calculada sobre o valor total atualizado da Ata de Registro de Preços, na hipótese de recusa injustificada do licitante vencedor em assinar a Ata de Registro de Preços e/ou retirar ou confirmar o recebimento da nota de empenho, no prazo máximo de 5 (cinco) dias úteis, após regularmente convocado, caracterizando inexecução total das obrigações acordadas;

d) Multa de 0,33% (zero vírgula trinta e três por cento) por dia de atraso, incidente sobre o valor total atualizado da contratação, pelo atraso injustificado para o

fornecimento/substituição de produtos/materiais, a ser cobrada pelo período máximo de 30 (trinta) dias. A partir do 31º (trigésimo primeiro) dia de atraso, a contratação será anulada e a Ata de Registro de Preços será cancelada;

e) Multa de 5% (cinco por cento) sobre o valor total atualizado da contratação, nos casos de anulação da contratação por culpa da contratada;

f) Multa de até 5% (cinco por cento) sobre o valor total atualizado da contratação quando for constatado o descumprimento de qualquer obrigação ou condição prevista neste Edital e/ou no Termo de Referência, em qualquer hipótese de inexecução total ou parcial, ou qualquer outra irregularidade na execução do objeto, ressalvadas aquelas obrigações para as quais tenham sido fixadas penalidades específicas, aplicada em dobro na reincidência.

19.3. A aplicação das sanções previstas neste Edital não exclui a possibilidade de aplicação de outras, previstas na Lei nº 8.666/93 e no Decreto nº 6.973/13, inclusive a responsabilização do licitante vencedor por eventuais perdas e danos causados à EMASA.

19.4. As multas aplicadas deverão ser recolhidas à EMASA, por meio de depósito em conta corrente, observando-se sua data de vencimento, podendo a Administração cobrá-las judicialmente, com os encargos correspondentes, ou descontá-las dos valores remanescentes de pagamentos à empresa.

20. DAS CONDIÇÕES DE CONTRATAÇÃO

20.1. **Quando for o caso, a licitante vencedora poderá ser convocada para assinar o contrato.**

20.2. **A convocação poderá ser realizada via comunicação eletrônica no email informado na proposta de preços.**

20.3. **Será obrigatória assinatura eletrônica do contrato, mediante uso da certificação digital, caso o representante legal da licitante não a possua, o prazo para regularização será de até 5 dias úteis após convocação.**

20.4. **Caso a licitante não compareça ou assine o contrato no prazo estabelecido, fica o Pregoeiro autorizado a convocar outra licitante para assumir o objeto da licitação e, após negociação e verificação da adequação da proposta e das condições de habilitação, assinar o respectivo contrato, obedecida a ordem de classificação.**

20.5. **Antes da assinatura o vencedor poderá também ser convocado para participar de reunião de inicial com o fiscal do contrato.**

20.6. **O prazo de convocação acima estabelecido poderá ser prorrogado uma vez, por igual período, quando solicitado pelo licitante vencedor durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração da EMASA.**

20.7. **A verificação de recebimento do email cabe ao exclusivamente ao licitante vencedor.**

20.8. A recusa injustificada da adjudicatária em assinar o contrato dentro do prazo fixado neste item caracterizará inadimplência das obrigações decorrentes desta licitação, sujeitando-se a mesma às penalidades previstas neste Edital e na legislação vigente.

20.9. Ocorrendo a hipótese do subitem anterior, o processo retornará ao(à) pregoeiro(a) e, que convocará os licitantes remanescentes e procederá ao exame das demais propostas, bem como da habilitação de seus ofertantes, segundo a ordem da classificação, até que uma proposta atenda integralmente ao Edital, sendo o seu autor declarado vencedor e convocado para assinar o contrato.

20.10. Para fins de assinatura de contrato, o licitante vencedor deverá apresentar documento que indique a composição societária da empresa vencedora, de sorte a comprovar a legitimidade de representação e, na hipótese de não ser sócio administrador da empresa, procuração que demonstre tratar-se de pessoa detentora de poderes para representá-la, bem como cópia autenticada de sua cédula de identidade.

21. DAS DISPOSIÇÕES GERAIS

21.1. **A EMASA não recebe documentos físicos (notas fiscais, certidões, relatórios, medições, etc). Todo recebimento de documentos se dará através de protocolo eletrônico. Sendo assim, o recebimento de mercadorias somente se efetivará após o pré-agendamento junto ao Setor de Almoxarifado, da Nota Fiscal e certidões devidamente anexadas ao protocolo eletrônico que deve ser aberto no sistema 1DOC. O fornecedor/entregador deverá informar o número do protocolo eletrônico na portaria da EMASA, no momento da entrega, para que sua entrada seja autorizada. A AUSÊNCIA DO DEVIDO PROTOCOLO ELETRÔNICO COM SEUS ANEXOS, IMPLICARÁ NA RECUSA DO RECEBIMENTO!**

20.1.1. **As notas fiscais e seus anexos devem ser protocoladas eletronicamente pelo site: https://emasa.1doc.com.br/atendimento**

20.1.2. **Cada protocolo deve conter apenas 01 (uma) nota fiscal.**

21.2. **PARA PROTOCOLAR AGENDAMENTO DE ENTREGA DE MATERIAIS, É IMPRESCINDÍVEL ANEXAR:**

20.2.1. **Nota fiscal;**

20.2.2. **Certidão Negativa de Débitos Federais;**

20.2.3. **Certificado de Regularidade do FGTS – CRF;**

20.2.4. **Autorização de Uso da nota fiscal eletrônica.**

21.3. **PARA PROTOCOLAR NOTA FISCAL DE SERVIÇOS É IMPRESCINDÍVEL ANEXAR:**

20.3.1. **Nota fiscal;**

20.3.2. **Relatório dos serviços prestados;**

20.3.3. **Certidão Negativa de Débitos Federais.**

20.3.4. **Certificado de Regularidade do FGTS - CRF.**

21.4. **A ausência da documentação supracitada poderá resultar em atrasos no pagamento. Questionamentos poderão ser efetuados no próprio protocolo eletrônico.**

21.5. **O Protocolo Eletrônico é a forma oficial de pré-agendamento de entrega de produtos, entrega de Notas Fiscais e documentos correlatos junto à EMASA.**

21.6. **Para tanto, além de anexar eletronicamente tais documentos, o fornecedor deverá fazer uma breve descrição do que será entregue, indicando, entre outros dados, o processo licitatório ou compra direta que gerou a contratação, conforme modelo inicial apresentado no campo "Descrição".**

21.7. **A EMASA poderá, a qualquer momento, dentro deste mesmo sistema eletrônico de protocolo de notas fiscais, vir a solicitar outros documentos, para que seja possível a liquidação da despesa e o seu consequente pagamento.**

21.8. **É de responsabilidade exclusiva do fornecedor, o acompanhamento on-line dos trâmites provenientes de seus processos eletrônicos.**

21.9. **O CARREGAMENTO E/OU DESCARGA DE MATERIAIS, PRODUTOS, OU EQUIPAMENTOS, É DE TOTAL RESPONSABILIDADE DO FORNECEDOR.**

21.10. **Dúvidas quanto aos procedimentos do protocolo eletrônico, podem ser sanadas através do telefone (47) 3261 0050.**

21.11. A participação no presente Pregão implica na aceitação integral e irretratável de todas as condições exigidas neste Edital e nos documentos que dele fazem parte, bem como na observância dos preceitos legais e regulamentares em vigor.

21.12. Será lavrada a ata da sessão pública de realização do Pregão, que registrará os fatos ocorridos e estará disponível aos participantes no sistema eletrônico.

21.13. Ao Diretor Geral da EMASA compete anular este Pregão por ilegalidade, de ofício ou por provocação de qualquer pessoa, bem como revogá-lo, em qualquer de suas fases, por considerá-lo inoportuno ou inconveniente diante de fato superveniente, mediante ato escrito e fundamentado, sem que caiba aos respectivos participantes direito à reclamação ou indenização.

21.13.1. A anulação do Pregão induz à da Ata de Registro de Preços, bem como à do Contrato.

21.14. As proponentes assumem todos os custos de preparação e apresentação de suas propostas e a EMASA não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

21.15. É facultado ao Pregoeiro ou à autoridade superior, em qualquer fase deste Pregão, promover diligência destinada a esclarecer ou completar a instrução do processo, vedada a inclusão posterior de informação ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação.

21.16. No julgamento das propostas e na fase de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos e a sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de classificação e habilitação.

21.17. Presumir-se-ão como aceitos, para todos os efeitos, os prazos definidos neste Edital e em seus respectivos anexos.

21.18. Em caso de divergência entre normas infra legais e as contidas neste Edital, prevalecerão as últimas.

21.19. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na EMASA.

21.20. Este Pregão poderá ter a data de abertura da sessão pública transferida por conveniência da EMASA, sem prejuízo do disposto no art. 4º, inciso V, da Lei nº 10.520/02.

21.21. Todo e qualquer esclarecimento pertinente a este Pregão será sanado exclusivamente por meio de endereço eletrônico: licitacao@emasa.com.br, **ou pelo Protocolo Eletrônico, disponível no site da EMASA**. Nenhum esclarecimento a respeito do Pregão será prestado por telefone.

21.22. O Departamento de Contratos e Licitações desconsiderará todos os e-mails que tratam de atividades sob responsabilidade de outros setores, tais como: recebimento de produtos e equipamentos, recebimento de notas fiscais, pagamentos. Os contatos para tratar destes assuntos devem ser direcionados exclusivamente para o(s) respectivo(s) setor(es) responsável(eis).

21.23. É facultado ao Pregoeiro autorizar que os licitantes façam ligações telefônicas durante o certame, bem como o tempo de duração das mesmas.

21.24. No início da sessão o(a) Pregoeiro(a) poderá deliberar a respeito do uso de aparelhos celulares, smartfones, notebooks, computadores e afins, durante a sessão.

21.25. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que sejam possíveis a aferição da sua qualificação e a exata compreensão de sua proposta, durante a realização da sessão pública de pregão.

21.26. À EMASA reserva-se o direito de revogar a presente licitação por razões de interesse público ou anulá-la por ilegalidade.

21.27. Cópia deste ato convocatório poderá ser obtida no site www.emasa.com.br.

21.28. A EMASA poderá emitir nota de esclarecimento para sanar eventuais dúvidas sobre este edital, a qual será publicada no site www.emasa.com.br junto ao edital.

21.29. **VISTORIA TÉCNICA**

21.29.1. É facultado às proponentes a realização de vistoria nos locais de execução dos serviços, a fim de obtenção de subsídios para a adequada elaboração de suas propostas comerciais.

21.29.2. A CONTRATANTE não aceitará quaisquer alegações posteriores relativas a desconhecimento das condições dos locais em que serão prestados os serviços como desculpa para o descumprimento de obrigações contratuais ou de exigências contidas neste termo de referência ou no Edital.

21.29.3. As licitantes se obrigam a declarar que têm pleno conhecimento das condições necessárias para a prestação dos serviços, objeto da licitação.

21.29.4. Durante a vistoria técnica, a licitante que encontrar algum aspecto incompatível com os termos do edital deverá comunicar formalmente e tempestivamente à Administração, a fim de que esta possa se manifestar também formalmente a respeito e em tempo hábil.

21.29.5. O silêncio da licitante importará a sua aceitação total e irrestrita a todos os termos do edital.

21.29.6. No caso da Realização de Vistoria, o Departamento da EMASA emitirá Declaração de Vistoria, assinada conjuntamente por servidor do Departamento e pelo representante da empresa, atestando que o licitante vistoriou as instalações, tomou conhecimento das condições locais e de todos os elementos técnicos necessários ao cumprimento do objeto da licitação, admitindo-se, consequentemente, como certo, o prévio e total conhecimento da situação.

21.29.7. Alternativamente, a licitante poderá apresentar declaração de renúncia de vistoria devidamente preenchida e assinada pelo seu representante legal, não sendo aceita alegações posteriores relativas a desconhecimento das condições dos locais do serviço como motivo para o descumprimento de obrigações contratuais ou de exigências contidas neste termo de referência ou no Edital.

21.29.8. A vistoria poderá ser agendada junto ao Departamento de Tecnologia da Informação, através do telefone (47) 3261-0000, das 12h00 às 17h00, de segunda a sexta feira, no prédio sede da EMASA.

21.29.9. A visita técnica poderá ocorrer até a véspera à data fixada para a realização da licitação.

Balneário Camboriú, 23 de novembro de 2022.

DOUGLAS COSTA BEBER ROCHA
Diretor Geral

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Registro de preço para eventual contratação de solução de segurança da informação para proteção inteligente de dados em repouso, estruturados e não estruturados, controle de acesso, visibilidade e rastreabilidade de utilização de dados em servidores de arquivos, banco de dados LOCAIS e na NUVEM, custódia de chaves criptográficas para ambientes em NUVEM (Pública, híbrida ou privada) composta por softwares e serviços de garantia e suporte técnico, serviços de instalação e configuração da solução, serviços de treinamento, serviços para integrações necessárias com soluções de terceiros e serviços especializados para atender às demandas da EMASA, conforme especificações técnicas e demais condições constantes deste Termo de Referência.

2. JUSTIFICATIVA

2.1. Nos últimos anos, é notável o aumento da complexidade do ambiente de TI da EMASA, uma vez que diversos novos sistemas e aplicações estão fazendo parte da rotina diária dos usuários internos e externos da EMASA. Com o aumento da complexidade e da demanda por serviços online, torna- se necessária a garantia de disponibilidade, integridade e performance dos sistemas, requerendo o máximo de disponibilidade, performance e integridade da informação armazenada por estes.

2.2. Este ambiente, complexo, se encontra em constante evolução seja por novas aquisições ou atualizações de seus componentes e remete a alguns desafios de governança, dentre eles o de conhecer e tratar eventuais falhas de segurança na forma de um processo continuado, visando antecipar riscos e agindo de forma proativa.

2.3. Tal fato, alinhado ao aumento de demandas por fornecimentos de serviços tecnológicos por parte dessa instituição através de sistemas online e a alta complexidade do parque de ativos de infraestrutura, maximiza o risco de vazamento de dados através da exploração de eventuais falhas de segurança não conhecidas presentes no ambiente tecnológico.

2.4. No tocante à proteção contra-ataques cibernéticos, como os ocorridos em diversos órgãos federais, estaduais e municipais ao longo dos últimos anos e inclusive nós com o ataque que sofremos, do tipo RANSOMWARE (sequestro de dados) e vazamento de dados confidenciais, uma solução de proteção dos dados é fundamental para preservar a integridade dos dados sensíveis, como ficha funcional e ou dados financeiros, da EMASA.

2.5. Cabe ainda ressaltar o comprometimento por parte deste órgão em atingir a conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa física ou por pessoa jurídica de direito público ou privado.

2.6. A presente contratação dos softwares e serviços que constam neste termo de referência, se faz necessária para que essa instituição assegure maiores índices de segurança em seu parque tecnológico e informações, recursos de anonimização e pseudonimização dos dados e custódia inteligente de chaves criptográficas face ao grande número de vazamento de dados que são reportados diariamente pelo portal ANPD.

2.7. Enquanto isso, regulamentações de proteção de dados e melhores práticas do setor conforme definido pela Cloud Security Alliance, exigem que as chaves sejam armazenadas e gerenciadas em ambiente diferente das operações de criptografia associadas. Os provedores podem atender requisitos, oferecendo serviços “Traga sua própria chave” (BYOK) para habilitar o controle do cliente das chaves usadas para criptografar seus dados.

2.8. A solução aqui descrita é fundamental para que a EMASA obtenha êxito na criação e manutenção de um processo contínuo de proteção de dados, seja em servidores de arquivos (dados em repouso), aplicações, banco de dados (dados estruturados) ou em ambientes em nuvem.

2.9. Sem um processo que proteja o dado, seja onde ele estiver, a EMASA estará sujeita a passar por incidentes de segurança com grave impacto ao desempenho institucional, tais como indisponibilidade nos serviços fornecidos, acesso e distribuição ilegal de informações e tempo investido pela equipe no tratamento e resposta de ocorrências.

2.10. Esta necessidade ampara-se ainda na determinação do Tribunal de Contas da União sobre Segurança da Informação que, dentre as quais, cita-se o Acórdão nº 1233/2012-TCU-Plenário, item 9.8:

“Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Gabinete de Segurança Institucional da Presidência da república (GSI/PR) que ... em atenção a Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II (subitem II.8)”.

2.11. Conclui-se da necessidade de aquisição de uma tecnologia que apoie o Departamento de Tecnologia da Informação na missão de proteger as informações (dados), implantando uma solução que impeça o acesso às informações por pessoas não autorizadas. Assim como pautar formalmente uma política de desastre e recuperação nesta Casa de Leis.

2.12. Ainda a justificar a contratação os benefícios esperados são:

a) Redução na quantidade de incidentes de segurança.
b) Proteção de dados em repouso, e atuação preventiva com relação a vazamento de dados.
c) Apoiar as demais áreas da EMASA no controle da segurança da informação.
d) Atingir conformidade com a Lei 13.709 – Lei Geral de Proteção de Dados e demais padrões de segurança recomendados para órgãos da administração pública, com a aplicação de medidas técnicas razoáveis para proteger dados pessoais/sensíveis, através de relatórios de acessos.
e) Criar um ambiente protegido para a administração dos dados, segregando as funções de administração de servidores/sistemas e administração de dados.
f) Viabilizar a estratégia de jornada para nuvem para garantir a Proteção de Dados, com custódia e controle de acesso exclusivamente a EMASA, com gestão e armazenamento seguro das chaves de criptografia, evitando perda de informações.
g) Esta contratação ainda visa auxiliar o Encarregado de Dados quanto a aplicação da LGPD;
h) Administração dos dados de forma centralizada, com visibilidade de relatórios.
i) Atuação preventiva com relação a vazamento de dados.

3. DA DESCRIÇÃO DA SOLUÇÃO, ESPECIFICAÇÕES TÉCNICAS E QUANTIDADES

3.1. Estimativa de Bens e Serviços previstos para a presente contratação:

Lote	ITEM	QTD	Unidade	Descrição da Solução	Métrica	VALOR MÉDIO UNIT - (ANUAL)	VALOR MÉDIO TOTAL (ANUAL)
1	1	4	UN	Fornecimento de agente para proteção de dados para aplicação multiplataforma	Software		
	2	1	UN	Fornecimento de agente para transferência segura de base de dados	Software		
	3	5	UN	Fornecimento de agentes de proteção de dados estruturados multiplataforma	Software		
	4	5	UN	Fornecimento de agentes de proteção de dados não estruturados multiplataforma	Software		
	5	1	UN	Fornecimento de agentes para descoberta e classificação de dados sensíveis - termo de licenciamento por 12 Meses - 15TB	Software		
	6	2	UN	Fornecimento de agentes para gestão de chaves local - 12 meses	Software		
	7	1	UN	Fornecimento de agentes para proteção e custódia de chaves multicloud – termo de licenciamento por 12 meses	Software		
	8	2	UN	Fornecimento de console de gerenciamento de chaves de criptografia em alta disponibilidade	Software		
	9	3	UN	Serviço de Treinamento oficial	Serviço		
	10	12	UN	Serviço de suporte técnico especializado (Helpdesk) – 12 meses	Serviço		
	11	5	UN	Serviço de suporte para agentes de proteção de dados estruturados multiplataforma – 12 meses	Serviço		
	12	5	UN	Serviço de suporte para agentes de proteção de dados não estruturados multiplataforma – 12 meses	Serviço		

	13	4	UN	Serviço de suporte para agentes de proteção de dados para aplicação multiplataforma – 12 meses	Serviço		
	14	2	UN	Serviço de suporte para agentes para gestão de chaves local – 12 meses	Serviço		
	15	2	UN	Serviço de suporte para console de gerenciamento de chaves de criptografia – 12 meses	Serviço		
	16	2	UN	Serviço de Implementação de console de gerenciamento de chaves de criptografia	Serviço		
	17	3000	UST	Serviço sob demanda para Implementação de agentes de criptografia	Serviço		
2	2	12	UN	Serviço de gestão de projetos e documentação - 12 meses	Serviço		
3	3	12	UN	Serviço de análise de risco - 12 meses	Serviço		
4	4	8	UN	Serviço de consultoria para avaliação periódica (HealthCheck)	Serviço		
5	5	12	UN	Serviço de consultoria sob demanda para emissão de relatórios de conformidade com a LGPD - 12 meses	Serviço		
6	6	12	UN	Serviço de diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico	Serviço		
7	7	1	UN	Serviço de suporte de solução para transferência segura de base de dados	Serviço		
					TOTAL		

3.2. DESCRIÇÃO DA SOLUÇÃO TECNOLÓGICA

3.2.1. A plataforma e/ou ferramental tecnológico deverá atender às seguintes especificações técnicas e requisitos de gestão:

3.2.2. A solução ofertada deve reduzir ao máximo a ocorrência de incidentes internos de segurança monitorando a atividade de credenciais com acessos privilegiados (ex. Administradores, root, etc.), bem como impedindo que estes usuários acessem o conteúdo dos dados. Isso tudo, sem que os mesmos percam privilégio para administrar o ambiente de tecnologia;

3.2.3. A solução ofertada deve estabelecer o controle de acesso para esse tipo de usuário e identificar atividades suspeitas gerando logs destas atividades;

3.2.3.1. A solução ofertada deve estabelecer um modelo de proteção para informações de tal forma que o dado seja devidamente criptografado no sistema de arquivos. Desta forma, além de impedir a extração não autorizada, mesmo em caso de vazamento acidental dos dados, deverá garantir que os dados não possam ser acessados fora do ambiente gerenciado pela plataforma de segurança, uma vez que não terão a chave de criptografia necessária para acessar a informação;

3.2.3.2. A solução ofertada deve prover mecanismos de prevenção de infecção ou ataques a arquivos por malware, APT, ransomware, ataques gerados por acesso não autorizado, modificações em bibliotecas entre outros, quando estes forem originados de usuários com acesso privilegiado;

3.2.3.3. A solução ofertada deve ser flexível e escalável, adequando-se às necessidades de crescimento da empresa contratante;

3.2.3.4. A solução ofertada precisa permitir a anonimização dos dados pessoais e/ou confidenciais,

conforme definido no artigo 12 da Lei Geral de Proteção de Dados Brasileira (LGPD);

3.2.3.5. A solução ofertada deve proteger sistemas de dados estruturado (bancos de dados) e sistemas de dados não estruturado (incluindo arquivos de aplicativos da Microsoft, voz, vídeo e texto em geral) em um ambiente heterogêneo de sistemas operacionais e plataformas de operação;

3.2.4. A solução ofertada deve suportar pelo menos:

3.2.4.1. Sistemas operacionais Microsoft Windows Server, e Linux;

3.2.4.2. Os bancos de dados suportados devem incluir MS-SQL, MySQL e arquivos;

3.2.4.3. Provedores de nuvem suportados devem incluir AWS S3, Azure, Office 365, e IBM Cloud;

3.2.4.4. A solução ofertada deve suportar tudo com console de gerenciamento centralizada para facilitar o processo de administração, controle de acesso, gestão e logs e manutenção da solução de proteção de dados;

3.2.4.5. Soluções baseadas em software livre não serão aceitas.

3.3. FORNECIMENTO DE CONSOLE DE GERENCIAMENTO DE CHAVES DE CRIPTOGRAFIA EM ALTA DISPONIBILIDADE

3.3.1 A solução deverá prover um console de gerenciamento composta por um conjunto integrado de produtos baseados em uma infraestrutura comum e extensível, com gerenciamento centralizado de políticas e de chaves, reduzindo o esforço de administração e o custo total de propriedade.

3.3.2 O Console de Gerenciamento deve oferecer recursos para proteger e controlar o acesso a dados estruturados e não estruturados hospedados em ambientes físicos e virtuais, ON PREMISES e na NUVEM.

3.3.3 A solução deve prover um console único que permita o gerenciamento centralizado de todos os agentes de criptografia, suas chaves de criptografia, políticas de configuração, publicação e controle de acesso dos dados a serem protegidos.

3.3.4 O console deve possuir certificação FIPS 140-2, Common Criteria, ou outra equivalente, para garantir total segurança das chaves de criptografia.

3.3.5 O console de gerenciamento centralizado deve suportar agentes para as funcionalidades que seguem:

3.3.6 Criptografia transparente – para criptografar, controlar o acesso ao dado e oferecer registros de auditoria de acesso aos dados sem impactar nas aplicações, base de dados ou infraestrutura onde quer que os servidores estejam instalados;

3.3.7 Integração com SIEM–suportar integração com os sistemas de gerenciamento de logs do mercado, como: Splunk, qRadar, Arcsight, McAfee, LogRhythm e etc;

3.3.8 Segurança de container - oferecer criptografia de dados, controle de acesso e registro de acesso ao dado;

3.3.9 Gerenciamento de chaves em nuvem múltipla – permitir custódia e controle de dados em ambiente de software como serviço (SaaS), relatório de acesso e eficiência no gerenciamento do ciclo de vida da chave em nuvem com o conceito Traga sua Própria Chave (BYOK);

3.3.10 Toquenização e mascaramento de dados - reduzir os custos e o esforço necessários para cumprir com as políticas de segurança e normas regulatórias como o LGPD, dentre outras;

3.3.11 Criptografia para aplicações – simplificar o processo de adição de criptografia em aplicações, por meio de Ais baseadas em padrões que potencializam operações criptográficas e de gerenciamento de chaves de alto desempenho.

3.3.12 O console deve ser capaz de ser configurado em alta disponibilidade (HA) com um servidor primário e outro secundário. A configuração de alta disponibilidade deve permitir a hospedagem dos servidores primário e secundário em datacenters distintos e conectados.

3.3.13 Apoiar a incorporação de vários consoles adicionais para fins de configuração de esquemas de tolerância a falhas multinível.

3.3.14 Os agentes instalados nos servidores devem operar de forma autônoma não causando impacto em caso de perda de comunicação com o console.

3.3.15 Os agentes devem fazer a rotação/mudança de chaves “a quente”, ou seja, sem indisponibilidade nos servidores de dados.

3.3.16 Cada console deve ter a capacidade de suportar o crescimento.

3.3.17 Detalhes da chave de criptografia não devem ser divulgados para usuários do sistema para que o algoritmo de criptografia esteja protegido dos usuários da plataforma. Estes devem ser armazenados de forma segura em um dispositivo virtual dedicado aos serviços de segurança dentro do console.

3.3.18 É desejável que todos os elementos da solução sejam do mesmo fabricante, porém serão aceitas soluções compostas por mais de um fabricante desde que estes fabricantes comprovem interoperabilidade e suporte a solução ofertada.

3.3.19 O console deve possuir capacidade de gerenciar chaves criptográficas padrão KMIP.

3.3.20 Deve ser compatível com API PKCS # 11 e Microsoft Key Extensible Management.

3.3.21 Deve ser capaz de oferecer suporte a certificados digitais (X. 509) PKCS # 7, PKCS # 8 e PKCS # 12, chaves de criptografia simétrica (algoritmos3DES, AES128, AES256, ARIA128 e ARIA256) e assimétrica (algoritmos RSA1024, RSA2048, RSA4096).

3.3.22 Deve ser escalável para oferecer suporte a gerenciamento de agente de vários serviços em uma estrutura de Multitenant e com suporte a configuração de segurança de vários domínios. Para isso, deve possibilitar configurar diferentes chaves criptográficas de acordo com cada área de operação, se necessário.

3.3.23 Quando aplicada a separação de funções, o console deve permitir que o usuário do sistema crie chaves de criptografia, outro usuário pode aplicá-las e outro, que não seja o anterior, consiga monitorar o mesmo durante a aplicação.

3.3.24 O console deve possibilitar gerenciamento via interface Web, possibilitar comandos (CLI) e API (SOAP, REST).

3.3.25 Deve requerer autenticação de usuário e senha e, opcionalmente, dois fatores RSA.

3.3.26 Deve ser capaz de configurar cópias de backup de suas configurações automaticamente ou manualmente.

3.3.27 Requerimentos complementares:

3.3.28 Suportar usuários múltiplos;

3.3.29 Escalabilidade comprovada para mais de 10.000 agentes;

3.3.30 Cluster para alta disponibilidade (HA);

3.3.31 Toolkit e interface de programação;

3.3.32 Integração infraestrutura de autenticação existente, com fácil configuração;

3.3.33 Suporte para API RESTfull;

3.3.34 Autenticação multi-fator;

3.3.35 Opções de instalação:

3.3.36 Sistema virtual com certificação FIPS 140-2 Nível, ou certificação compatível;

3.3.37 O sistema virtual deve ser compatível com VMware ou Hyper-V.

3.4. **FORNECIMENTO DE AGENTES DE PROTEÇÃO DE DADOS ESTRUTURADOS MULTIPLATAFORMA.**

3.4.1. Este agente deve fornecer criptografia de banco de dados (dados 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. O agente deverá residir no sistema operacional ou na camada de dispositivo, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela.

3.4.2. O processo de criptografia deve ser executado por agentes que serão instalados nos servidores de banco de dados.

3.4.3. Esses agentes devem oferecer suporte a sistemas operacionais Microsoft, e/ou Linux.

3.4.4. Eles devem ser compatíveis com bancos de dados estruturados e não estruturados, incluindo MS-SQL Server, MySQL.

3.4.5. Deve ser compatível com servidores físicos e versões virtualizadas.

3.4.6. Sua implementação não deve exigir qualquer alteração no banco de dados ou na aplicação.

3.4.7. Estes devem usar os recursos de aceleração disponíveis, como o AES-NI. A implementação

destes não deve gerar uma carga incremental, típica em servidores, de mais de 5%.

3.4.8. Além de criptografar o banco de dados, os agentes devem ser capazes de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações estruturadas e não estruturadas (por exemplo: imagens, vídeos, arquivos voz, syslog, etc.).

3.4.9. Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso.

As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio.

Essas diretivas devem permitir e serem baseadas em usuário, processo, tipo de arquivo e agendamento.

3.4.10. As políticas devem poder ser aplicadas aos usuários locais, ou igualmente integradas no AD ou no LDAP.

3.4.11. Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com o console de gerenciamento, para poder aplicar processos de criptografia e descriptografia.

3.4.12. Os logs de atividade do usuário devem poder de ser enviados para uma solução de SIEM através de um servidor de syslog ou no formato CEF, em tempo real e nativamente.

3.4.13. A solução deve suportar ambiente em nuvem, tais como AWS, Azure, pelo menos.

3.4.14. A solução deve ter a capacidade de integrar os serviços de gerenciamento de chaves fornecendo serviços de gerenciamento de chaves no local ou na nuvem, para aplicações como Salesforce.com.

3.4.15. Registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos.

3.4.16. Possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados.

3.4.17. Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não criptografado.

3.4.18. Requerimentos complementares:

3.4.19. Compatibilidade com os sistemas operacionais:

3.4.20. Windows Server: 2008, 2012 e posteriores.

3.4.21. Windows: 7; 8,1, 10 e posteriores.

3.4.22. Linux: RedHat; CentOS, Ubuntu e Debian.

3.4.23. Permitir criptografia para múltiplos fabricantes de banco de dados, tais como:

3.4.24. MySQL (Windows, Linux);

3.4.25. MS SQL (Windows).

3.4.26. FORNECIMENTO DE AGENTE PARA TRANSFERÊNCIA SEGURA DE BASE DE DADOS

3.4.27. Este agente deve permitir o mascaramento dos dados sensíveis para permitir o compartilhamento seguro com terceiros, ambientes de teste, ambientes de desenvolvimento e outros casos de uso aplicáveis.

3.4.28. O funcionamento deve ser baseado em tabela e/ou coluna. Informa-se o que deverá ser mascarado no novo banco de dados de destino. Com isso, dados não identificados podem ser compartilhados.

3.4.29. A solução de ser customizável e de alta performance.

3.4.30. A solução deve suportar, pelo menos, as operações de criptografia / tokenização e descriptografia / destokenização de tabelas e / ou colunas.

3.4.31. A solução deve ser transparente para a aplicação ou banco de dados com acesso via conexão ODBC. Ou seja, não deve requerer alterações ou instalações adicionais no servidor de banco de dados.

3.4.32. A solução deve suportar, pelo menos, arquivo CSV, Microsoft SQL Server, MySQL.

3.4.33. A solução deve permitir replicação de arquivo para arquivo, banco de dados para banco de dados, arquivo para banco de dados e banco de dados para arquivo.

3.4.34. Pelo menos os seguintes modelos devem ser suportados: Standard AES Encryption, Batch random Tokenization e Batch FPE FF3/FF1.

3.4.35. FORNECIMENTO DE AGENTES DE PROTEÇÃO DE DADOS NÃO ESTRUTURADOS MULTIPLATAFORMA.

3.4.36. Este agente deve fornecer criptografia de servidor de arquivo (dado não estruturado) 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. O agente deverá residir no sistema operacional ou na camada de dispositivo, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela.

3.4.37. O processo de criptografia deve ser executado por agentes que deverão ser instalados nos servidores de arquivos.

3.4.38. Os agentes devem oferecer suporte a sistemas operacionais Microsoft e/ou Linux.

3.4.39. Deve ser compatível com servidores físicos e versões virtualizadas.

3.4.40. Sua implementação não deve exigir qualquer alteração no servidor de arquivo ou processo para manuseio do dado pelo usuário final.

3.4.41. Deve ser capaz de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações não estruturadas (por exemplo: imagens, vídeos, arquivos

voz, syslog, etc.).

3.4.42. Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso.

3.4.43. As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio.

3.4.44. Essas diretivas devem permitir serem baseadas em usuário, processo, tipo de arquivo e agendamento.

3.4.45. As políticas devem ser aplicadas aos usuários locais, ou igualmente integradas no AD ou no LDAP.

3.4.46. Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com o console de gerenciamento para poder aplicar processos de criptografia e descriptografia.

3.4.47. Os logs de atividade do usuário devem ter a capacidade de ser enviado para uma solução de SIEM através de um servidor de syslog ou no formato CEF, em tempo real e nativamente.

3.4.48. A solução deve suportar ambiente em nuvem, tais como AWS, Azure, pelo menos.

3.4.49. Registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos.

3.4.50. Possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados.

3.4.51. Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não criptografado.

3.4.52. Compatibilidade com os sistemas operacionais:

3.4.53. Windows Server: 2016 e superiores.

3.4.54. Windows: 10 e superiores.

3.4.55. Linux: RedHat 7-6; CentOS, Ubuntu e Debian.

3.5. **FORNECIMENTO DE AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO MULTIPLATAFORMA.**

3.5.1 Este agente deve permitir a toquenização vaultless com o Dynamic Data Masking, para eficientemente Anonimizar dados, incluindo dados pessoais, quer eles residem on premises, ambientes de big data ou a nuvem. Com isso, reduzir o escopo de conformidade substituindo dados confidenciais por um token não-sensível que olha e age como o original. Ou seja, proteção de dados sem a necessidade de alterar bancos de dados. Depois que os dados confidenciais são substituídos pelo token, os sistemas não estão mais sujeitos a conformidade, significando menos esforço para atender regulamentações.

3.5.2 Possuir alto desempenho com baixo impacto na performance da aplicação.

3.5.3 Possuir servidores de token virtual escalável.

3.5.4 Comunicação via TLS autenticado mutuamente.

3.5.5 Interface REST API com chamadas individuais e em lote.

3.5.6 Permitir geração de Tokens Aleatórios.

3.5.7 Compatível com FPE FF1, Tokens FF3.

3.5.8 Permitir Mascaramento Dinâmico ou Estático de Dados.

3.5.9 Gerenciamento de chaves e políticas.

3.5.10 Suporte AD / LDAP.

3.5.11 Suporte a dados numéricos e alfanuméricos.

3.5.12 Permitir a criação de tokens em formatos numéricos, de texto e de data para aplicativos únicos ou múltiplos.

3.5.13 Permitir utilizar grupos de usuários LDAP para decidir quais informações são exibidos para grupos específicos. Por exemplo, operadoras de call center versus gerentes de call center.

3.5.14 Suportar servidor de tokens no formato virtual de sua escolha: OVF, ISO, Microsoft Azure Marketplace ou Amazon AMI.

3.5.15 Restringir o acesso a ativos confidenciais sem alterar os esquemas do banco de dados, sem interrupções.

3.5.16 Proteger dados em trânsito e em repouso.

3.5.17 Mascarar os dados em ambiente de desenvolvimento, teste e terceirizados com acesso ao banco de dados.

3.5.18 Proteger DBAs, administradores de sistema, root, e usuários mal-intencionados com acesso direto ao banco, uma vez que os dados que este irão acessar não são dados reais.

3.6. **FORNECIMENTO DE AGENTES PARA PROTEÇÃO E CUSTÓDIA DE CHAVES MULTICLOUD.**

3.6.1 A Este agente deve prover o controle de chave pelo próprio cliente permitindo a separação, criação, propriedade, controle e revogação das chaves de criptografia sem a dependência do provedor. Deverá reduzir a complexidade do gerenciamento de chaves, dando ao próprio cliente controle de ciclo de vida de chaves de criptografia com gerenciamento centralizado, visibilidade e rastreabilidade.

3.6.2 Deverá cumprir com os regulamentos de proteção de dados e armazenamento de chaves rigorosos, podendo chegar a FIPS 140-2 Nível 3, ou certificação equivalente.

3.6.3 Prover eficiência com gerenciamento de chave centralizado em ambientes de nuvem híbrida.

3.6.4 Fornecer acesso a cada provedor de nuvem a partir de uma única janela do navegador, incluindo várias contas ou assinaturas.

3.6.5 Rotacionar de forma automática as chaves para cumprir com regulamentações que exigem este serviço de rotação de chave.

3.6.6 Fornecer mecanismos simples, via login federado, para conceder acesso aos dados. Com isso, ser compatível com logins de serviços em nuvem que são autenticados e autorizados pelo provedor de serviços, isto é, nenhum banco de dados de login nem configuração AD ou LDAP é necessário.

3.6.7 Fornecer meios para solicitar a criação de chaves nos provedores de nuvem e fornecer gerenciamento completo do ciclo de vida das mesmas.

3.6.8 Controlar e gerenciar centralizadamente várias nuvens, IaaS e SaaS (Multicloud).

3.6.9 Prover registro (log), rastreabilidade e relatórios de conformidade totalmente independente do provedor de nuvem.

3.6.10 O agente deve suportar, pelo menos, os provedores de nuvem que seguem:

3.6.11 Microsoft Azure;

3.6.12 Microsoft Office365;

3.6.13 Amazon Web Services.

3.7. **FORNECIMENTO DE AGENTES PARA GESTÃO DE CHAVE LOCAL.**

3.7.1 Ser capaz de centralizar o gerenciamento de chaves de aplicativos de terceiros que usam criptografia nativa, tal como bancos de dados.

3.7.2 O agente deve ter a capacidade de conectar-se com os aplicativos por meio de interfaces padrão e fornecer acesso às funções robustas de gerenciamento de chaves.

3.7.3 Prove simplificação e redução da carga operacional por meio do gerenciamento centralizado de chaves.

3.7.4 Elevar o nível de segurança pela separação das chaves de criptografia das aplicações, banco de dados, storage e etc.

3.7.5 Gerenciar chave utilizando soluções de hardware ou software com certificação FIPS ou equivalente.

3.7.6 Suportar o protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP / PKCS) que é o padrão do setor para troca de chaves de criptografia entre clientes (usuários principais) e um servidor (armazenamento de chaves). A padronização simplifica o gerenciamento de chaves externas.

3.7.7 Garantir a custódia de chaves para, pelo menos:

3.7.8 A Oracle TDE;

3.7.9 SQL TDE;

3.7.10 Nutanix;

3.7.11 VMWare;

3.7.12 Cisco;

3.7.13 Netapp;

3.7.14 Certificados;

3.7.15 Aplicações desenvolvidas em casa;

3.7.16 Outros volumes compatíveis.

3.8. **FORNECIMENTO DE AGENTES PARA DESCOBERTA E CLASSIFICAÇÃO DE DADOS SENSÍVEIS.**

3.8.1 A solução deverá possibilitar a descoberta de dados, em ambiente de dados estruturados e não estruturados, armazenados em diferentes repositórios, tais como:

3.8.2 Servidores de Arquivos;

3.8.3 Bancos de Dados;

3.8.4 Estações de trabalho.

3.8.5 A solução deve permitir, através de interface única, realizar o levantamento e entendimento dos dados existentes, sua localização e riscos associados, permitindo:

3.8.6 Atender aos requisitos de privacidade;

3.8.7 Obter visibilidade sobre os dados que estão em risco de exposição;

3.8.8 Suportar a criação de plano de privacidade e proteção de dados.

3.8.9 A solução ofertada deverá possibilitar, pelo menos, quatro níveis de classificação de dados por padrão:

3.8.10 Restrito;

3.8.11 Privado;

3.8.12 Interno;

3.8.13 Público.

3.8.14 A solução deve atribuir pontuações de risco que permitam identificar o nível de sensibilidade dos dados, como arquivos e bancos de dados, agregando os seguintes parâmetros:

3.8.15 Nível de proteção;

3.8.16 Quantidade de elementos encontrados;

3.8.17 Localização;

3.8.18 Quantidade de dados confidenciais.

3.8.19 As pontuações de risco devem permitir identificar os dados com maior exposição e permitir priorizar medidas de proteção.

3.8.20 A solução deve suportar os seguintes ambientes:

3.8.21 Armazenamento local em Hard Disk e Memória dos computadores;

3.8.22 Armazenamentos em rede;

3.8.23 Compartilhamento Windows CIS e SMB;

3.8.24 Network File System NFS;

3.8.25 Bancos de Dados:

3.8.26 SQL.

3.8.27 A solução deve suportar os seguintes tipos de arquivos:

3.8.28 Banco de Dados:

3.8.29 Access;

3.8.30 Dbase;

3.8.31 SQLite;

3.8.32 MSSQL MDF & LDF.

3.8.33 Arquivos de Imagens:

3.8.34 BMP;

3.8.35 FAX;

3.8.36 GIF;

3.8.37 JPG;

3.8.38 PDF;

3.8.39 PNG;

3.8.40 TIF.

3.8.41 Arquivos Compactados:

3.8.42 bzip2;

3.8.43 Gzip (todos os tipos);

3.8.44 TAR;

3.8.45 Zip (todos os tipos).

3.8.46 Microsoft Backup:

3.8.47 Microsoft Binary / BKF.

3.8.48 Microsoft Office: v5, 6, 95, 97, 2000, XP, 2003 e superiores.

3.8.49 Open Source:

3.8.50 Star Office;

3.8.51 Open Office.

3.8.52 Padrões abertos:

3.8.53 PDF;

3.8.54 HTML;

3.8.55 CSV;

3.8.56 TXT.

3.8.57 A solução deve classificar os dados como:

3.8.58 Dado pessoal;

3.8.59 Dados financeiros, com base em modelos integrados ou técnicas de classificação.

3.8.60 Deve possibilitar a identificação de informações padronizadas do Brasil, tais como:

3.8.61 Registro Geral (RG);

3.8.62 CPF;

3.8.63 CNH;

3.8.64 Passaporte.

3.8.65 A solução deve permitir a inclusão de modelos de políticas (descoberta e classificação) específicas para LGPD.

3.8.66 A solução deve fornecer relatórios detalhados para demonstrar conformidade com a Lei Geral de Proteção de Dados (LGPD).

3.8.67 A solução deve possibilitar a classificação de dados utilizando:

3.8.68 Regex,

3.8.69 Patterns,

3.8.70 Algoritmos,

3.8.71 Contexto.

3.8.72 A solução deve permitir ser implementada “com” ou “sem” agentes instalados.

3.8.73 A solução deve possuir as seguintes características funcionais:

3.8.74 Políticas: definir as políticas de privacidade de dados, locais e perfis de varredura e de classificação;

3.8.75 Descoberta: localizar dados estruturados e não estruturados, através de toda a organização em ambientes big data, banco de dados e sistema de armazenamento de arquivos;

3.8.76 Classificação: classificar dados pessoais e sensíveis, baseado em modelos pré-configurados e técnicas de classificação;

3.8.77 Análise de risco: entender a natureza do dado e seus riscos, oferecendo visualizações;

3.8.78 Relatórios: gráficos e relatórios de análise de risco, status e alertas durante todo o ciclo de vida do dado.

3.9. **SERVIÇO DE TREINAMENTO OFICIAL.**

3.9.1 O treinamento de capacitação técnica será ministrado para até 8 participantes selecionados pela EMASA, com carga horária mínima de 16 (dezesseis) horas, material oficial do fabricante, e conteúdo necessários a capacitá-los para utilizar o Sistema ofertado.

3.9.2 Deverá ser emitido certificado de participação ao final do curso.

3.9.3 Todo o material didático deve ser repassado de forma impressa e em mídia para os alunos.

3.9.4 Somente serão aceitos materiais oficiais dos fornecedores do Sistema ofertado, e não será permitida a adaptação sobre apostilas/conteúdos de cursos não oficiais.

3.9.5 Os instrutores deverão possuir experiência em didática, além de possuir certificação comprovada na área de segurança, em pelo menos uma das seguintes certificações:

3.9.6 ISC2 CSSLP - Certified Secure Software Lifecycle Professional (ISO/IEC 17024);

3.9.7 ISC2 CISSP – Certified Information System Security Professional;

3.9.8 ISC2 ISSAP – Information System Security Architect Professional;

3.9.9 CISM – Certified Information Security Manager;

3.9.10 CompTIA Security+: Competency in system security, network infrastructure, access control and organizational security.

3.9.11 O treinamento deverá ocorrer nas dependências da CONTRATANTE, ou local por ela indicado na capital do estado, ficando responsável por montar o ambiente adequado para realização do mesmo, isto é, todo o espaço necessário assim como toda infraestrutura computacional e de rede necessária. Caberá à CONTRATADA instalar a solução ou possibilitar o acesso ao Sistema no ambiente de treinamento.

3.9.12 Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento e hospedagem, a confecção e distribuição dos originais do material didático e a emissão de certificados para os profissionais treinados.

3.10. **SERVIÇO DE CONSULTORIA PARA AVALIAÇÃO PERIÓDICA (HEALTHCHECK).**

3.10.1 O Serviço deverá rever a implementação existente, validando as suas políticas de operação e proteção. Estes elementos serão avaliados contra as melhores práticas de mercado e as políticas específicas do cliente. Todos os procedimentos operacionais, e configurações deverão ser avaliados e documentados para garantir a estabilidade de integridade e tolerância a falhas.

3.10.2 O Serviço deverá contemplar toda a solução implementada desde as consoles até os agentes de proteção de dados.

3.10.3 Deverá ser executado mediante emissão de ordens de serviço.

3.10.4 Deverá ser executado periodicamente de não excedendo o intervalo de dois meses entre as execuções.

3.10.5 O Serviço deverá ser executado nas dependências do cliente, prioritariamente, em horário comercial. Caso o CLIENTE julgue necessário poderá ser agendada uma janela de manutenção fora do horário comercial sem custos adicionais para a contratante.

3.10.6 As Seguintes atividades deverão ser cobertas pelo serviço:

3.10.7 Verificar a configuração da solução, versão instalada e os requisitos de atualização, provendo relatório de impacto e orientação de planejamento para atualização;

3.10.8 Verificar a configuração de alta disponibilidade e status de replicação;

3.10.9 Verificar os procedimentos para fail-over;

3.10.10 Verificar os procedimentos de backup e restauração da plataforma, e as configurações do custodiante da chave;

3.10.11 Verificar as configurações de contas de administradores e domínios em relação aos requisitos de segurança;

3.10.12 Verificar os níveis e configurações de log atuais, a integração com quaisquer ferramentas SIEM e fornecer qualquer orientação sobre melhorias;

3.10.13 Verificar se as melhores práticas para backup automático e chaves estão implementadas e documentadas;

3.10.14 Identificar quaisquer políticas atualmente no modo de aprendizagem e o impacto potencial de permanecer nesse estado;

3.10.15 Avaliar e verificar os procedimentos gerais de implantação para criar e atualizar políticas e verificar a eficácia geral das políticas;

3.10.16 Analisar as configurações de log da solução e fazer as recomendações para eliminar mensagens de log desnecessárias e reduzir o número de logs que a solução precisa processar;

3.10.17 Demonstrar e executar relatórios que podem ser usados para verificar os resultados;

3.10.18 Revisar os procedimentos de atualização dos agentes de proteção instalados, como políticas de criptografia, configuração de hosts e instalação dos agentes;

3.10.19 Revisar os procedimentos operacionais existentes ou procedimentos de implantação de melhores práticas definidos e fazer recomendações e alterações conforme necessário;

3.10.20 Emitir relatório de status de saúde geral (HealthCheck) do ambiente contemplando, no mínimo, todos os itens de revisão e verificação.

3.10.21 Ao término da execução dos serviços de “HealthCheck” os relatórios deverão serão apresentados à contratada em mídia eletrônica para emissão do termo de aceite da ordem de serviço.

3.11. **SERVIÇO DE CONSULTORIA SOB DEMANDA PARA EMISSÃO DE RELATÓRIOS DE CONFORMIDADE COM A LGPD.**

3.11.1 O Serviço deverá realizar uma varredura no ambiente protegido pela solução identificando, neste ambiente, todos os pontos de não-conformidade com a LGPD.

3.11.2 O Serviço deverá contemplar toda a solução implementada desde os consoles até os agentes de proteção de dados.

3.11.3 O Serviço deverá ser executado nas dependências do cliente, prioritariamente, em horário comercial. Caso o CLIENTE julgue necessário poderá ser agendada uma janela de manutenção fora do horário comercial sem custos adicionais para a contratante.

3.11.4 As seguintes atividades deverão ser cobertas pelo serviço:

3.11.5 Verificar a configuração do agente de descoberta e classificação de dados, versão instalada e os requisitos de atualização, provendo relatório de impacto e orientação de planejamento para atualização;

3.11.6 Verificar as configurações de classificação de dados, fazendo as recomendações de melhorias;

3.11.7 Verificar a programação de varredura implementada, comparando com as políticas de segurança da contratante;

3.11.8 Verificar os logs das últimas varreduras identificando ocorrências de falhas e gerando recomendações para correções;

3.11.9 Avaliar as configurações de classificação de dados pessoais / sensíveis de acordo com a LGPD e suas atualizações, quando ocorrerem;

3.11.10 Realizar a varredura em todo ambiente atendido pela solução de proteção;

3.11.11 Gerar relatório de riscos e painéis gráficos;

3.11.12 Gerar relatório de conformidade com a LGPD;

3.11.13 Gerar recomendações de correção;

3.11.14 Emitir relatório consolidado da varredura com a evidência de todas as atividades realizadas, Painel de conformidade e lista de recomendações.

3.11.15 Ao término da execução dos serviços de “Consultoria sob demanda para emissão de relatórios de conformidade com a LGPD” o (s) relatório (s) deverão ser apresentados à contratada em mídia eletrônica para emissão do termo de aceite da ordem de serviço.

3.11.16 SERVIÇO DE GESTÃO DE PROJETOS E DOCUMENTAÇÃO

3.11.17 Resumo do Projeto, Apresentação, Objetivos, Benefícios, Responsabilidades, Recomendações, Premissas e Restrições;

3.11.18 Gerenciamento do escopo, declaração do escopo, plano de entrega, regras mudanças de escopo

3.11.19 Gerenciamento do Cronograma e prazos do projeto, bem como gestão dos recursos a serem utilizados

3.11.20 Gestão de Recursos Humanos alocados no projeto, definição comitê projeto

3.11.21 Responsabilidades do Comitê do Projeto

3.11.22 Gerenciamento de Riscos do Projeto e mitigação dos mesmos

3.11.23 Gerenciamento da Qualidade, métricas e metas de qualidade, lista de verificação de qualidades, documentação de entregas

3.11.24 Matriz de obrigatoriedade de documentos e artefatos a serem disponibilizados

3.11.25 Gerenciamento das Comunicações e documentação dos projetos

3.11.26 Diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico;

3.11.27 **Detalhamento Do Plano de Projeto**

3.11.28 A CONTRATADA deverá designar um profissional responsável pela gestão do projeto sendo esse o único ponto de contato com a CONTRATANTE;

3.11.29 Após a assinatura do contrato, com prazo máximo de 5 (cinco) dias úteis, a

CONTRATADA deverá informar o nome, telefone e e-mail do Gerente de Projetos e agendar a data da reunião inicial de projeto (Kick-off meeting);

3.11.30 A reunião inicial de projeto deverá seguir a seguinte pauta:

3.11.31 Apresentação das equipes CONTRATADA e CONTRATANTE;

3.11.32 Apresentação do Detalhamento do Plano de Projeto – Projeto Executivo

3.11.33 Aprovação do Plano do Projeto, após essa etapa iniciar a execução do projeto conforme o plano do projeto – Projeto Executivo

3.11.34 Detalhamento do plano do Projeto Executivo – Gestão de Projetos

3.11.35 Resumo do Projeto, Apresentação, Objetivos, Benefícios, Responsabilidades, Recomendações, Premissas e Restrições;

3.11.36 Gerenciamento do escopo, declaração do escopo, plano de entrega, regras mudanças de escopo

3.11.37 Gerenciamento do Cronograma e prazos do projeto, bem como gestão dos recursos a serem utilizados

3.11.38 Estabelecimento de cronograma executivo;

3.11.39 Gestão de Recursos Humanos alocados no projeto, definição comitê projeto

3.11.40 Estabelecimento da lista de contatos e funções definindo claramente.

3.11.41 Responsáveis técnicos por cada equipe, profissionais responsáveis pelas definições técnicas do projeto;

3.11.42 Executivos de cada equipe, profissionais responsáveis pelos aspectos operacionais, jurídicos e financeiros do projeto;

3.11.43 Analistas de cada equipe, profissionais envolvidos nas diversas atividades de projeto;

3.11.44 Responsabilidades do Comitê do Projeto

3.11.45 Estabelecimento da matriz de relacionamentos;

3.11.46 Estabelecimento da matriz de responsabilidades identificando quem executa, quem precisa ser informado, quem avalia, quem aprova e quem aceita formalmente o resultado em nome da CONTRATANTE.

3.11.47 Gerenciamento de Riscos do Projeto e mitigação dos mesmos

3.11.48 Gerenciamento da Qualidade, métricas e metas de qualidade, lista de verificação de qualidades, documentação de entregas

3.11.49 Matriz de obrigatoriedade de documentos e artefatos a serem disponibilizados

3.11.50 Gerenciamento das Comunicações e documentação dos projetos

3.11.51 Estabelecimento do plano de comunicação entre as equipes de forma que todos estejam atualizados em relação às diversas atividades de projeto;

3.11.52 Estabelecimento do formato e dos meios de troca de informações entre as equipes da CONTRATADA e da CONTRATANTE;

3.11.53 Definição da agenda das reuniões de acompanhamento de projeto.

3.12. **SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO (HELP DESK)**

3.12.1 A CONTRATADA deverá possuir um processo de Help-Desk;

3.12.2 Nível 1

3.12.3 Realizar triagem para correta identificação de problemas;

3.12.4 Prover atendimento via telefone, web, e-mail, chat e acesso remoto à equipamentos (quando disponível);

3.12.5 Elaborar relatórios técnicos específicos;

3.12.6 Solucionar dúvidas referentes ao comportamento, comandos, facilidades e características;

3.12.7 Esclarecer dúvidas sobre mensagens de erro;

3.12.8 Prestar Suporte técnico durante as mudanças;

3.12.9 Nível 2

3.12.10 Prover atendimento especializado para ocorrências complexas;

3.12.11 Solucionar problemas analisando a causa raiz e propondo planos de ações para evitá-los no futuro;

3.12.12 Prover informações e recomendações para melhoria dos serviços;

3.12.13 Contribuir para a base de conhecimento;

3.12.14 Os profissionais da CONTRATADA executará todas as configurações e customizações necessárias para o pleno funcionamento do ambiente, proporcionando as condições para transferência de know-how;

3.12.15 Esse serviço deverá ser realizado de forma presencial para assegurar que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos em regime 8 x 5 em horário comercial (08:00 às 18:00);

3.12.16 A qualidade dos serviços deverá ser assegurada através de processos consolidados e da sólida formação, capacitação e experiência dos profissionais responsáveis pelas atividades;

3.12.17 OS profissionais da CONTRATADA deverão execução os processos customização de configurações e mudanças, seja em decorrência de alarmes e processos e também por solicitação da CONTRATANTE;

3.12.18 Os profissionais da CONTRATADA deverão executar as atividades operacionais, utilizando os procedimentos estabelecidos para cada rotina;

3.12.19 Os profissionais da CONTRATADA deverão executar as atividades de manutenção corretiva, utilizando os procedimentos que permitam maior eficiência e eficácia na solução de falhas

3.12.20 Os profissionais da CONTRATADA deverão executar as atividades de manutenção

preventiva, rotinas de testes, análises e medidas, utilizando os procedimentos que assegurem mínima interferência na operação e máxima disponibilidade da plataforma

3.12.21 Os profissionais da CONTRATADA deverão elaborar procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário;

3.12.22 As customizações e regras das diversas plataformas serão executadas mediantes chamados específicos obedecendo o SLA acordado;

3.12.23 Os profissionais da CONTRATADA deverão elaborar relatórios de atividades detalhando os procedimentos realizados e eventuais ajustes, se necessário;

3.12.24 A CONTRATADA deverá prestar o apoio -técnico para campanhas de segurança para usuários finais, em conjunto com as áreas internas da CONTRATANTE, em especial para as áreas de Tecnologia da Informação e Recursos Humanos, para esclarecimento de usuários sobre os riscos e sobre as boas práticas de segurança digital;

3.12.25 A CONTRATADA deverá disponibilizar informações técnicas para preparação de material de palestras e informativos, bem como as métricas obtidas através da própria plataforma para ilustração dos principais riscos detectados e mitigados;

3.12.26 Os profissionais da CONTRATADA deverão promover a manutenção de *appliances* e equipamentos dedicados fornecidos pela CONTRATADA;

3.13. **SERVIÇO DE ANÁLISE DE RISCO - SAR**

3.13.1 Planejamento do gerenciamento de risco

3.13.2 Identificação dos riscos

3.13.3 Realização de análise quantitativa (Probabilidade)

3.13.4 Realização da análise Qualitativa (impacto)

3.13.5 Planejar resposta aos riscos

3.13.6 Controlar os riscos

3.13.7 Fazer levantamento de ameaças, coletando informações acerca dos seus processos de tecnologia buscando pelas principais ameaças que possam ser claramente identificadas:

3.13.8 Perda de dados;

3.13.9 Incêndio em data center

3.13.10 software desatualizados;

3.13.11 sistemas fora do ar;

3.13.12 colaboradores sem treinamento;

3.13.13 Excesso de usuários privilegiados.

3.13.14 Sistemas operacionais desatualizados.

3.13.15 Criação de matriz de risco formada por dois eixos: a probabilidade da ocorrência do risco e o impacto que ele trará caso ocorra.

3.13.16 Eixo da probabilidade:

3.13.17 Quase certo: é praticamente impossível evitar que o risco aconteça, por isso vale a pena pensar em ações de mitigação do impacto do risco depois dele ocorrer;

3.13.18 alta: a chance de o risco ocorrer é grande e frequentemente ele ocorre de fato;

3.13.19 média: probabilidade ocasional de acontecimentos do risco. Ainda vale a pena planejar desdobramentos, mas não com tanta preocupação como nos casos anteriores;

3.13.20 baixa: pouca chance de acontecer algum problema advindo desse risco;

3.13.21 Rara: É bastante improvável que o risco aconteça, só vale a pena se preocupar em casos de impacto grave ou gravíssimo para o seu projeto.

3.13.22 Eixo do impacto:

3.13.23 Gravíssimo: pode fazer com que o projeto seja cancelado ou que o dano ocasionado por ele seja irreversível;

3.13.24 Grave: compromete de forma acentuada o resultado do projeto, ocasionando atraso ou insatisfação do cliente;

3.13.25 médio: perda momentânea ao longo do projeto que pode ser corrigida, mas com o impacto no escopo ou no prazo;

3.13.26 Leve: desvio quase imperceptível dos objetos do projeto ser facilmente corrigido;

3.13.27 Sem impacto: não gera nenhum tipo de problema perceptível para o projeto, por isso pode ser ignorado em 99% dos casos. Só dê atenção se esse risco ocorrer quase com certeza e com alta frequência.

3.14. **SERVIÇO DE DIAGNÓSTICO, AVALIAÇÃO, MAPEAMENTO E LEVANTAMENTO DO PARQUE TECNOLÓGICO**

3.14.1. Executar diagnóstico de conformidade sobre o ambiente tecnológico do cliente.

3.14.2. Executar levantamento de parque tecnológico, com todas as suas características:

3.14.2.1. Quantidade de servidores de arquivos (dados não estruturados).

3.14.2.1.1. Qual a versão do sistema operacional (SO) dos Servidores (Windows, Linux e etc)

3.14.2.2. Quantidade de servidores de banco de dados (dados estruturados).

3.14.2.2.1. Qual as versões dos Sistemas operacionais (SO) dos servidores. (Windows, Linux e etc).

3.14.2.2.2. Quais os Banco de dados existentes (Oracle, Mysql, Sql e etc).

3.14.2.3. Executar levantamento por serviço de aplicação que faz chamadas " API REST" Mapeamento de dados sensíveis e seus fluxos de interação entre usuários e dados não estruturados, aplicação/usuários e dados estruturados pré e pós implantação.

3.15. **SERVIÇO DE SUPORTE PARA CONSOLE DE GERENCIAMENTO E SEUS AGENTES DE PROTEÇÃO.**

3.15.1. Suporte técnico 24x7.

3.15.2. Troubleshooting problemas de comunicação com os agentes.

3.15.3. Escalação de problemas para as áreas responsáveis de Administração e Operação.

3.15.4. Atuação em chamados de problemas e incidentes abertos no Help Desk.

3.15.5. Atualização dos chamados.

3.15.6. Apoio e esclarecimento de causa raiz do problema.

3.15.7. Detalhamento da solução adotada.

3.15.8. Documentação de evidências.

3.15.9. Confecção de relatórios mensais da saúde e principais eventos do gerenciamento.

3.15.10. Disposições gerais dos Serviços

3.15.10.1. Caberá a CONTRATANTE, disponibilizar o ambiente tecnológico para que a solução da CONTRATADA seja instalada e configurada;

3.15.10.2. Caberá a CONTRATANTE, disponibilizar os profissionais adequados para fornecer todas as informações necessárias para o desenvolvimento dos serviços;

3.15.10.3. Caberá a CONTRATANTE, informar todos os parâmetros técnicos necessários para que a solução da CONTRATADA seja instalada e configurada;

3.15.10.4. Caberá a CONTRATANTE, disponibilizar ambiente de trabalho adequado para os profissionais da CONTRATADA poderem executar os serviços. Esse ambiente será composto por mesa, cadeira e acesso à rede da CONTRATANTE;

3.15.10.5. A CONTRATADA deverá manter ao longo da vigência do contrato, profissionais qualificados com experiência relacionada às atividades propostas;

3.15.10.6. A contratada, deverá utilizar metodologia e sistema de controle de acesso de forma a possibilitar o rastreamento;

3.15.10.7. A contratada deverá aplicar os conceitos de segurança em telecomunicações, redes e Internet de acordo com as melhores práticas de mercado;

3.15.10.8. A contratada deverá aplicar práticas de Gestão de Segurança e Criptografia de forma a manter o sigilo das informações da CONTRATANTE;

3.15.10.9. A contratada deverá aplicar da melhor forma possível o tratamento da informação que terá acesso mantendo a Confidencialidade, Integridade e Disponibilidade das informações;

3.15.10.10. Os profissionais da contratada deverão prestar atendimento em língua portuguesa;

3.15.10.11. A CONTRATADA deverá prover por meio do mesmo canal de Suporte Técnico Especializado, o atendimento às consultas sobre as falhas de segurança identificadas pela plataforma ou qualquer um dos itens fornecidos, prover auxílio ao tratamento de incidentes encontrados e melhores práticas aplicáveis às medidas recomendadas, além de dirimir dúvidas sobre o ambiente monitorado;

3.15.10.12. 0 nível de serviço de suporte técnico terá caráter reativo no que diz respeito às solicitações de usuários do Sistema, e preventivo no que diz respeito às atualizações e melhorias em eventuais características ou funcionalidades da solução, e deverá ser prestado

remotamente de forma a assegurar os níveis de disponibilidade para manter a solução de segurança ofertada em perfeitas condições de uso;

3.15.10.13. Os serviços de Operação da Plataforma serão prestados pelo período de 12 (doze) meses;

3.15.10.14. A CONTRATANTE, poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência do contrato, para suprir suas necessidades com relação à Plataforma de Segurança;

3.15.10.15. Os serviços de Operação da Plataforma, exceto Service Desk, deverão ser prestados presencialmente nas dependências da CONTRATANTE seguindo o regime 24x7x365 atendendo aos seguintes requisitos:

3.15.10.16. Local de atendimento: CONTRATANTE;

3.15.10.17. Atendimento presencial: De segunda-feira à sexta-feira exceto feriados;

3.15.10.18. Atendimento remoto: todos os dias da semana incluindo fins de semana e feriados;

3.15.10.19. Horário de atendimento presencial: das 8:00 às 18:00;

3.15.10.20. Horário de atendimento remoto: 24 horas por dia;

3.15.10.21. Se necessário, a CONTRATANTE fornecerá credenciais de acesso para os profissionais da CONTRATADA. Essas credenciais serão individuais, não podendo ser compartilhadas entre os profissionais da CONTRATADA. Tais acessos serão auditados;

3.15.10.22. CONTRATANTE deverá emitir o termo de recebimento provisório referente ao serviço de Instalação dos Hardwares, Softwares e Licenças da Plataforma em até 5 (cinco) dias úteis após a entrega do "Relatório de Implementação", e o termo de recebimento definitivo em até I O (dez) dias úteis;

3.15.10.23. Após a assinatura do termo de aceite definitivo fica a CONTRATADA autorizada a emitir a Nota Fiscal relativa aos serviços de implantação;

3.15.10.24. Para fins de comprovação da execução dos serviços mensais de Operação, a CONTRATADA deverá entregar até o quinto dia útil do mês subsequente juntamente com a Nota Fiscal o relatório mensal contendo:

3.15.10.25. Relação dos tickets de atendimento realizados no período;

3.15.10.26. Relação das atividades realizadas no período, contendo, quando couber:

3.15.10.27. Rotinas executadas;

3.15.10.28. Relação das atividades de manutenção preventiva, rotinas de testes, análises e medidas executados;

3.15.10.29. Relação de procedimentos elaborados;

3.15.10.30. Relação de incidentes de segurança que ocorreram no período, contendo:

3.15.10.31. Data e hora da ocorrência;

3.15.10.32. Descrição da ocorrência;

3.15.10.33. Impacto/risco para o negócio;

3.15.10.34. Pessoal notificado;

3.16. ***DEMAIS SERVIÇOS COMPLEMENTARES:***

3.17. **FORNECIMENTO DAS LICENÇAS.**

3.17.1. O fornecimento das licenças que compõem a solução deverá ocorrer por intermédio de ordem de empenho.

3.17.2. A CONTRATADA terá o prazo de 5 (cinco) dias úteis para realizar a entrega das licenças a partir da data de emissão da ordem de fornecimento de bens.

3.17.3. As licenças deverão ser fornecidas na forma de certificado nomeadas a EMASA, e com os respectivos números de série.

3.17.4. Na ocasião do fornecimento das licenças, deverão ainda ser entregues os aplicativos instaladores (executáveis/binários) acompanhados de documentação técnica em formato digital (manuais de operação) de cada software que compõe a solução;

3.17.5. AS licenças serão de 12 meses podendo ser renováveis.

3.18. **INSTALAÇÃO E CONFIGURAÇÃO.**

3.18.1. A implantação da solução será realizada por intermédio da abertura de Ordem de Serviço específica.

3.18.2. As seguintes atividades fazem parte de seu escopo:

3.18.2.1. Elaboração de plano de instalação, contendo todos os requisitos técnicos, etapas, prazos e matriz de responsabilidades;

3.18.2.2. Instalação da solução todos os módulos que a compõe, no ambiente disponibilizado pela EMASA;

3.18.2.3. Configurações necessárias para emissão de alertas através do sistema de correio eletrônico da EMASA;

3.18.2.4. Integração com NOC da EMASA.

3.18.3. Caberá a EMASA disponibilizar o ambiente tecnológico para que a solução da CONTRATADA seja instalada e configurada.

3.18.4. O prazo máximo para a execução do serviço é de 30 (trinta) dias úteis, a contar da data em que a EMASA disponibilizar o ambiente e credenciais de acesso para a execução da instalação e configurações.

3.18.5. Ao término da execução do serviço, a CONTRATADA deverá elaborar um relatório com evidência de todo o processo de instalação, e ceder credenciais de acesso à equipe da EMASA.

3.18.6. O serviço de instalação e configuração da solução foi estimado como atividade de ocorrência única, posto que uma vez concluído, servirá como base para todos os outros serviços que fazem parte do escopo do contrato.

3.18.7. A instalação e configuração da plataforma deverá ser realizada nas dependências da EMASA, em horário comercial.

3.19. **MANUTENÇÃO, SUPORTE TÉCNICO E GARANTIA.**

3.19.1. A CONTRATADA deverá disponibilizar o canal de suporte técnico, através de serviço telefônico, por no mínimo, 8x5 (oito horas por dia, cinco dias por semana), com atendimento, obrigatoriamente em língua portuguesa, falada no Brasil, devendo operar, no mínimo, em dias úteis no horário comercial, das 8h (oito horas) às 18h (dezoito horas), horário de Brasília.

3.19.2. A CONTRATADA deverá fornecer suporte técnico no Brasil, obrigatoriamente em língua portuguesa, falada no Brasil para prestar atendimento e resolver todos os problemas relacionados às possíveis falhas ou interrupções de funcionamento da solução proposta, sempre que solicitado pela EMASA;

3.19.3. A CONTRATADA deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da EMASA. De modo a assegurar alta disponibilidade do canal de suporte técnico para o Sistema fornecido, o registro de chamados deve estar disponível em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados).

3.19.4. Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

3.19.5. A EMASA poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência do contrato, para suprir suas necessidades com relação aos produtos de segurança.

3.19.6. Para efeito de avaliação dos níveis de serviços prestados no suporte técnico, considerar-se-á a contagem de tempo de atendimento apenas para os chamados abertos no curso do período de atendimento, em horário comercial, de modo que os chamados abertos foram deste período serão contabilizados apenas a partir do início do período útil operacional seguinte.

3.19.7. Relatórios sobre a prestação dos serviços:

3.19.7.1. A contratada fornecerá relatórios mensais sobre a prestação dos serviços, em papel e em arquivo eletrônico, preferencialmente em formato PDF, com informações analíticas e sintéticas sobre os serviços realizados, incluindo-se chamados abertos e fechados, enfatizando aqueles resolvidos no período.

3.19.7.2. Constarão dos relatórios dados de todos os chamados ocorridos no período, data e hora de abertura do chamado, data e hora de início do atendimento, data e hora de fechamento do chamado, nome da pessoa que abriu o chamado, nome da pessoa que efetuou o atendimento, descrição do problema e descrição da solução.

3.19.7.3. Também devem constar dados da reabertura de chamados, quando for o caso, que

foram fechados sem serem devidamente resolvidos e que, por esse motivo, necessitaram ser reabertos.

3.19.7.4. Deverá ainda apresentar relatório para cada solicitação de suporte remoto, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes.

3.19.8. Os atendimentos das ocorrências técnicas devem ser realizados em acordo com os critérios definidos pelos níveis de serviço da tabela abaixo, estando sujeita a CONTRATADA, no caso do descumprimento dos prazos, às sanções especificadas a seguir:

	NÍVEL DE SEVERIDADE DO CHAMADO			
	BAIXA	**MÉDIA**	**ALTA**	**URGENTE**
Descrição do chamado	Problema técnico que gere pouco ou baixo impacto na utilização da solução.	Problema técnico que impeça a utilização parcial de uma funcionalidade, não impedindo por completo seu uso.	Problema técnico que impeça completamente a utilização de uma funcionalidade.	Problema técnico que impeça a utilização da solução em sua totalidade.
Prazo para atendimento da ocorrência	Até 12 horas úteis	Até 8 horas úteis	Até 4 horas úteis	Até 0,5 horas úteis

3.19.9. Sempre que o fabricante da solução disponibilizar versões mais atuais da solução oferecida, a licitante deverá fornecer estas versões e releases dos softwares da solução para a EMASA, sem ônus adicionais, enquanto o contrato estiver vigente.

3.19.10. Entende-se por manutenção corretiva a série de procedimentos destinados ao restabelecimento operacional da solução com todas suas funcionalidades, motivados pela ocorrência de incidentes na solução e/ou problemas recorrentes na solução, compreendendo, inclusive, atualização de softwares por um substituto de igual ou maior configuração, ajustes, reparos, correções necessárias;

3.19.11. Entende-se por suporte técnico aquele efetuado mediante atendimento telefônico ou remoto, para resolução de problemas e esclarecimentos de dúvidas sobre a configuração e utilização da solução.

3.19.12. Os serviços deverão ser realizados por meio de técnicos especializados, devidamente credenciados para prestar os serviços de garantia e assistência técnica remoto, de forma

rápida, eficaz e eficiente, sem quaisquer despesas adicionais para a EMASA, inclusive quanto às ferramentas, equipamentos e demais instrumentos necessários à sua realização.

3.20. **DESCRIÇÃO DOS SERVIÇOS ESPECIALIZADOS.**

3.20.1. O fornecimento dos serviços especializados objeto deste certame observará o seguinte quantitativo:

Item	Descrição	Unidade	Quantidade
23	SERVIÇOS SOB DEMANDA PRA IMPLEMENTAÇÃO DE AGENTES DE CRIPTOGRAFIA	UST	3.000

3.20.2. Os serviços especializados tratam da operacionalização da gestão de chaves criptográficas, com apoio presencial de pessoal especializado ou remoto caso definido pela EMASA, devendo ser solicitado mediante emissão de ordem de serviço, informando às aplicações que farão parte do escopo do serviço.

30.20.3. Todas as atividades desempenhadas relativas aos serviços especializados deverão ser executadas nas dependências da EMASA, respeitando o horário de funcionamento da EMASA, e com o acompanhamento e ciência dos servidores.

3.20.4. Os serviços especializados serão demandados de acordo com a necessidade da EMASA, de forma proporcional ao número de agentes de criptografia instalados, mensurados através da métrica de UST, considerando que uma hora de trabalho equivale a uma UST.

3.20.5. Dada as diferentes atividades que compõem os serviços especializados, foram definidos três níveis de complexidade que visam garantir o equilíbrio físico-financeiro de sua execução, conforme disposto na tabela abaixo:

Nível de Complexidade	Definição
Normal	Cada hora de trabalho equivale a uma UST.
Média	Cada hora de trabalho equivale a duas UST's
Alta	Cada hora de trabalho equivale a três UST's.

3.20.6. Os serviços especializados deverão ser executados por colaboradores da CONTRATADA, respeitando as normas de segurança da informação da EMASA, executando as atividades observando criteriosamente o escopo definido nas respectivas ordens de serviços.

4. FORMAÇÃO DE PREÇO, DAS QUANTIDADES E VALORES DOS OBJETOS

4.1. A contratação dos equipamentos, software, aplicativo e serviços será feita sob demanda,

mediante autorização de fornecimento emitida pela CONTRATANTE;

4.2. A formação de preço, foi realizada com base nos orçamentos recebidos, sendo que o critério utilizado foi o preço médio. A tabela apresenta o resultado da pesquisa de preço;

4.3. A estimativa da despesa é RESTRITA. O Lote 1 contendo aquisição dos sistemas, licenças e serviços de suporte ao sistema contratado assim garantindo a integração. Os demais lotes (2, 3, 4, 5, 6 e 7) consistem em prestações de serviços.

Lote	ITEM	QTD	Unidade	Descrição da Solução	Métrica	VALOR MÉDIO UNIT - (ANUAL)	VALOR MÉDIO TOTAL (ANUAL)
1	1	4	UN	Fornecimento de agente para proteção de dados para aplicação multiplataforma	Software		
	2	1	UN	Fornecimento de agente para transferência segura de base de dados	Software		
	3	5	UN	Fornecimento de agentes de proteção de dados estruturados multiplataforma	Software		
	4	5	UN	Fornecimento de agentes de proteção de dados não estruturados multiplataforma	Software		
	5	1	UN	Fornecimento de agentes para descoberta e classificação de dados sensíveis - termo de licenciamento por 12 Meses - 15TB	Software		
	6	2	UN	Fornecimento de agentes para gestão de chaves local - 12 meses	Software		
	7	1	UN	Fornecimento de agentes para proteção e custódia de chaves multicloud – termo de licenciamento por 12 meses	Software		
	8	2	UN	Fornecimento de console de gerenciamento de chaves de criptografia em alta disponibilidade	Software		
	9	3	UN	Serviço de Treinamento oficial	Serviço		
	10	12	UN	Serviço de suporte técnico especializado (Helpdesk) – 12 meses	Serviço		
	11	5	UN	Serviço de suporte para agentes de proteção de dados estruturados multiplataforma – 12 meses	Serviço		
	12	5	UN	Serviço de suporte para agentes de proteção de dados não estruturados multiplataforma – 12 meses	Serviço		
	13	4	UN	Serviço de suporte para agentes de proteção de dados para aplicação multiplataforma – 12 meses	Serviço		
	14	2	UN	Serviço de suporte para agentes para gestão de chaves local – 12 meses	Serviço		
	15	2	UN	Serviço de suporte para console de gerenciamento de chaves de criptografia – 12 meses	Serviço		
	16	2	UN	Serviço de Implementação de console de gerenciamento de chaves de criptografia	Serviço		
	17	3000	UST	Serviço sob demanda para Implementação de agentes de criptografia	Serviço		
2	2	12	UN	Serviço de gestão de projetos e documentação - 12 meses	Serviço		
3	3	12	UN	Serviço de análise de risco - 12 meses	Serviço		
4	4	8	UN	Serviço de consultoria para avaliação periódica (HealthCheck)	Serviço		
5	5	12	UN	Serviço de consultoria sob demanda para emissão de relatórios de conformidade com a LGPD - 12 meses	Serviço		
6	6	12	UN	Serviço de diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico	Serviço		
7	7	1	UN	Serviço de suporte de solução para transferência segura de base de dados	Serviço		

TOTAL		

4.4. Os itens serão adquiridos sob demanda para efetivação do contrato.

4.5. Alguns dos itens poderão não serem contratados.

5. DAS CONDIÇÕES DE ENTREGA E EXECUÇÃO

5.1. Nos termos dos artigos 73 a 76 da Lei 8.666/1993, o objeto do presente TERMO DE REFERÊNCIA será recebido:

5.1.1. Provisoriamente, pela Comissão de Recebimentos, no ato da entrega, para posterior verificação da conformidade dos produtos e/ou serviços com as especificações;

5.1.2. Se for constatada desconformidade do(s) produtos e serviços apresentados(s) em relação às especificações, o CONTRATADO deverá efetuar a troca ou correção, no prazo estabelecido neste termo de referência, a contar do recebimento da solicitação.

5.1.3. Neste caso, o recebimento do(s) produto(s) e/ou serviços escoimado(s) dos vícios que deram causa a sua troca será considerado recebimento provisório, ensejando nova contagem de prazo para o recebimento definitivo.

5.1.4. Definitivamente, no prazo de 30 (trinta) dias, contados do recebimento provisório, após criteriosa inspeção e verificação e análise por Comissão de Recebimento, a ser designada, de que os bens ou serviços a serem adquiridos encontram-se em perfeitas condições de utilização, além de atenderem às especificações do objeto contratado.

5.2. O aceite/aprovação do(s) produto(s) ou serviço(s) pelo órgão licitante não exclui a responsabilidade civil do CONTRATADO por vícios de quantidade ou qualidade do(s) produto(s) ou disparidades com as especificações estabelecidas, verificadas, posteriormente, garantindo-se a EMASA as faculdades previstas no art. 18 da Lei n.º 8.078/90.

5.3. A inspeção pode gerar a recusa de artefatos por motivo de vícios de qualidade ou por não observância dos padrões adotados pela EMASA.

5.4. Caso seja necessário, a substituição do produto deverá ocorrer no prazo de 10 (dez) dias.

5.5. A entrega deverá ser, obrigatoriamente, entre às 12h00 e às 17h00, de segunda à sexta-feira.

5.6. A entrega da mercadoria deverá ser feita somente após autorização do recebimento através do protocolo realizado pela empresa fornecedora, além disso, a carga e/ou descarga é de total responsabilidade do fornecedor. A autorização da entrega se dará mediante "*Protocolos Eletrônicos*" no site da EMASA devidamente regular conforme orientação enviada junto a nota de empenho;

5.7. Local de entrega de materiais, após agendamento via protocolo, se dará junto ao Almoxarifado da ETA – Estação de Tratamento de Água, situada na Av. Marginal Leste, n° 3350, Bairro dos Estados, Balneário Camboriú, CEP: 88339-125. De segunda a sexta-feira das 08h às 17h.

5.8. O fornecedor no momento da entrega, deverá apresentar número do protocolo. Na ausência desta informação, implicará no não recebimento da mercadoria.

5.9. A entrega/início dos serviços se dará através do fiscal do contrato ou pessoa designada.

6. CLASSIFICAÇÃO DOS BENS COMUNS E ADJUDICAÇÃO

6.1. O objeto a ser contratado enquadra-se na **categoria de Serviços Comuns**, de que tratam a Lei nº 10.520/02 e do Decreto nº 10.024/2019, por possuir padrões de desempenho e características gerais e específicas que podem ser definidos de forma objetiva nas especificações técnicas, que são usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da **Modalidade Pregão – Registro de Preços**, na forma de execução indireta sob o regime de empreitada por **Menor Preço por Lote.**

6.2. O decreto 7.892, de 23 de janeiro de 2013, que disciplina o sistema de registro de preços, define as hipóteses especiais, porém não taxativas, sobre a admissão do registro de preços pela administração pública.

6.3. A aquisição através de Sistema de Registro de Preços, disciplinado pelo art. 15, inciso II e §§ 1º a 6º da Lei nº 8.666/93 e regulamentado pelo Decreto nº 7.893/2013, possibilitará o atendimento da demanda de forma conjunta, após a adjudicação e a homologação do resultado da licitação pela autoridade competente, finalizando assim o procedimento estabelecido para o registro de preços mediante Ata de Registro de Preços, a ser firmada com a licitante vencedora para efeito de compromisso de fornecimento para futura contratação.

6.4. A ata de registro de preços, durante sua validade, poderá ser utilizada por qualquer órgão ou entidade da administração pública que não tenha participado do certame licitatório mediante anuência do órgão gerenciador, desde que devidamente justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas na Lei nº. 8.666, de 1993 e no Decreto nº. 7.892, de 2013.

6.5. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.

6.6. As aquisições ou contratações adicionais a que se refere este item não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

6.7. As adesões à ata de registro de preços são limitadas, na totalidade, ao quíntuplo do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que eventualmente aderirem.

6.8. Ao órgão não participante que aderir à ata competem os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação as suas próprias contratações, informando as ocorrências ao órgão gerenciador.

6.9. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços.

6.9.1. Caberá ao órgão gerenciador autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência da ata, desde que solicitada pelo órgão não participante.

6.10. O uso da Ata de Registro de Preços por qualquer órgão ou entidade da administração justifica-se, naturalmente, pela economia obtida por não incorrer essas instituições em gastos gerados nos processos licitatórios. Ademais, as ações adotadas por este Regional podem ser convenientes a outros órgãos ou entidades da administração.

6.11. No caso da contratação pleiteada neste certame, o Registro de Preços é necessário uma vez que a contratação poderá ser realizada por diferentes órgãos da Administração Pública, órgãos participantes ou não, com manifestação prévia ou posterior de interesse, por ocasião do mecanismo de compras conjuntas, assim como viabiliza a aquisição parcelada do objeto, frente ao cenário orçamentário restritivo atual.

6.12. O agrupamento dos itens em lote único levou em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competividade, uma vez que existem no mercado várias empresas com capacidade de fornecer os produtos na forma em que estão agrupados neste TR. O agrupamento encontra ainda justificativa em decisões já deliberadas pelo TCU sobre a matéria, tais como, o informativo 106 do TCU que traz decisão que “A aquisição de itens diversos em lotes deve estar respaldada em critérios justificantes“, adotando o entendimento do acórdão 5260/2011 – TCU – 1a câmara, de 06/07/2011, que decidiu que “Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si”.

6.13. Para organizar e alcançar maior economia de escala no processo de aquisição, visando resultado com maior vantajosidade para esta administração, vez que o aumento de quantitativos geram a consequente redução de preços a serem pagos.

6.14. Para facilitar a execução e fiscalização do contrato, propiciando maior nível de controle pela Administração, sendo prática comum reconhecida pelo mercado.

6.15. Ademais, a própria EMASA, já se manifestou no sentido de que, no caso específico, nas hipóteses de licitação com diversidade de objetos, o entendimento tem sido o de que o parcelamento ou não do objeto da licitação deve ser auferido sempre no caso concreto,

perquirindo-se essencialmente acerca da viabilidade técnica e econômica do parcelamento e da divisibilidade do objeto, conforme se vê no Acórdão nº 732/2008, o TCU se pronunciou no sentido de que "a questão da viabilidade do fracionamento deve ser decidida com base em cada caso, pois cada obra tem as suas especificidades, devendo o gestor decidir analisando qual a solução mais adequada no caso concreto".

6.16. Considerando o caso concreto a divisão desta licitação em lotes, afetaria a qualidade dos serviços, bem como a entrega efetiva da solução que se pretende contratar, desta feita, ressalta-se que não é possível o parcelamento ou a divisibilidade em razão da própria natureza do objeto.

6.17. Assim posto, resta claro que o agrupamento dos itens em lote único não é opcional, mas sim, estritamente necessário a aquisição de elementos de forma agrupada, sejam eles de serviços ou produtos, não cabendo assim, o fatiamento do fornecimento de outra forma, que o apresentado neste documento.

7. DA SUBCONTRATAÇÃO

7.1. Dispõe a Lei nº 8.666/93, em seu art. 72, que a CONTRATADA, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar partes do serviço ou fornecimento, até o limite admitido, em cada caso, pela Administração. A subcontratação, desde que prevista no instrumento convocatório, possibilita que terceiro, que não participou do certame licitatório, realize parte do objeto.

7.2. Será admitida a subcontratação do item de Serviço de Treinamento Oficial (3.11) sendo uma parcela a qual exige-se uma qualificação quanto a formação do objeto. Este limite deverá compreender os limites mínimo e máximo de 5% e ~~50~~10%, respectivamente, do valor total do contrato, nas seguintes condições:

7.2.1. É vedada a sub-rogação completa ou da parcela principal da obrigação. São obrigações adicionais da contratada, em razão da subcontratação:

7.2.2. Apresentar a documentação de regularidade fiscal das microempresas e empresas de pequeno porte subcontratadas, sob pena de rescisão, aplicando-se o prazo para regularização previsto no § 1º do art. 4º do Decreto nº 8.538, de 2015;

7.2.3. 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;

7.2.4. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, bem como pela padronização, pela compatibilidade, pelo gerenciamento centralizado e pela qualidade da subcontratação,

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. Não será aplicável a exigência de subcontratação quando a licitante for qualificada como microempresa ou empresa de pequeno porte.

8. DA PROPRIEDADE INTELECTUAL

8.1. A CONTRATADA deverá entregar a EMASA toda e qualquer documentação gerada em função da prestação de serviços, objeto desta contratação.

8.2. A CONTRATADA cederá a EMASA, em caráter definitivo, o direito patrimonial dos resultados produzidos durante a vigência do Contrato, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

8.3. A CONTRATADA fica proibida de veicular e comercializar os produtos e informações geradas, relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da EMASA.

9. DA GARANTIA

9.1. A contratada deverá apresentar a garantia de execução contratual de 5% (cinco por cento), sobre o valor global da contratação, em uma das modalidades previstas no §1º do art. 56 da Lei nº 8.666/93, no momento da assinatura do contrato.

10. FORMA DE PAGAMENTO

10.1. A(s) nota(s) fiscal(is)/fatura(s) somente deverá(ao) ser apresentada(s) para pagamento após a conclusão da etapa do recebimento, indicativo do cumprimento pela CONTRATADA de todas as obrigações pertinentes ao objeto contratado.

10.2. Ainda que a nota fiscal/fatura seja apresentada antes do prazo definido para recebimento, o prazo para pagamento somente fluirá após o efetivo atesto do recebimento definitivo.

10.3. A(s) nota(s) fiscal(is)/fatura(s) deverá(ao) estar acompanhadas da documentação probatória pertinente, relativa ao recolhimento dos impostos relacionados com a obrigação.

10.4. Em havendo alguma pendência impeditiva do pagamento, a exemplo de erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como obrigações financeiras pendentes, decorrentes de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus

para o CONTRATANTE.

10.5. Fica desde já reservado a EMASA o direito de não efetuar o pagamento se no ato da entrega e aceitação dos produtos/serviços estes não estiverem em perfeitas condições de conservação e consumo e de acordo com todas as especificações contidas neste Termo de Referência;

10.6. As Notas Fiscais deverão ser protocoladas para pagamento somente após a aprovação/atesto do produto pela EMASA.

10.7. O pagamento se dará em até 30 (trinta) dias de acordo com o recebimento da documentação exigida por completo e poderá ser acompanhado pela Contratante através do protocolo aberto pela mesma.

10.8. A CONTRATADA deverá protocolar as Notas Fiscais/Faturas seguindo o tramite:

10.8.1. 1º Passo: Acessar o link: https://emasa.1doc.com.br/atendimento e a opção "Protocolos Eletrônicos";

10.8.2. 2º Passo: Criar um login de acesso em nome da empresa usando CNPJ;

10.8.3. 3º Passo: No campo "Assunto" escolher a opção: "2200 - Notas Fiscais/Pré-agendamento de entrega de serviços comuns e produtos";

10.8.4. 4º Passo: Informar o número dos empenhos e anexar os documentos pertinentes.

10.9. AS NOTAS FISCAIS DEVEM SER ENVIADAS EXCLUSIVAMENTE VIA PROTOCOLO ELETRÔNICO DESCRITO ACIMA, E A RESPONSABILIDADE PELA APRESENTAÇÃO DA NOTA FISCAL NO PRAZO CORRETO, JUNTAMENTE COM OS DOCUMENTOS NECESSÁRIOS, É TODA DO FORNECEDOR.

11. DOS CRITÉRIOS DE ELABORAÇÃO DA PROPOSTA COMERCIAL

11.1. A proposta da licitante deverá conter a especificação clara dos bens e serviços, obedecida a mesma ordem constante deste Termo de Referência, sem conter alternativas de preços, ou de qualquer outra condição que induza o julgamento a ter mais de um resultado.

11.2. A proposta da licitante deverá estar integralmente preenchida, discriminando os valores unitários e totais dos bens e serviços objeto deste Termo de Referência.

11.3. A proposta deverá conter declaração da licitante de que se encontra apta a prestar todos os serviços pertinentes ao objeto ofertado.

11.4. A licitante deverá fornecer a proposta de acordo com a ordem prevista ano item 4 deste TR

11.5. A licitante deverá apresentar ainda, juntamente com sua proposta:

11.5.1. catálogo, folder, prospectos, fotos ou folhetos ilustrativos, ou manual técnico elaborado pela fabricante, ou documento extraído de consulta realizada pela internet, devendo, nesse caso, ser indicado o endereço eletrônico, que possibilite uma análise clara e inequívoca sobre as características do objeto ofertado.

12. DOS REQUISITOS NECESSÁRIOS

12.1. A licitante vencedora deverá apresentar, para sua qualificação técnico operacional, na fase de habilitação, atestado de Capacidade Técnica, emitido por pessoa jurídica de direito público ou privado, que comprove a aptidão da empresa proponente no desempenho de atividades compatíveis e de natureza semelhante em características com o objeto desta licitação, atestando, inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais, no(s) atestado(s) deverão estar contemplados, no mínimo, as seguintes parcelas de maior relevância e valor significativo:

12.1.1. Fornecimento/licenciamento de Solução de Gerenciamento e Segurança da Informação para proteção de dados em repouso e em trânsito, controle de acesso, visibilidade e rastreabilidade de utilização em servidores de arquivo, banco de dados, utilizando custódia de chaves criptográficas composta por software e hardware.

12.1.2. Fornecimento/licenciamento de software/solução de Gerenciamento de Segurança da informação (segurança digital), contemplando ferramenta de Criptografia e serviço de instalação configuração, capacitação e integração.;

12.2. O(s) atestado(s) deverá(ão) conter o nome das empresas declarantes, a identificação do nome e a assinatura do responsável, bem como o número de telefone para contato.

12.3. O (s) atestado(s) deverá(ão) estar acompanhados de cópias dos respectivos contratos/Notas Fiscais, bem como demais documentos comprobatórios do efetivo fornecimento.

12.4. Para efeito de qualificação técnico profissional, na fase de habilitação, a licitante deverá apresentar, documento que ateste possuir pelo menos 1 profissional com certificação CISSP (Certified Information Systems Security Professional) ou CISM (Certified Information Security Manager), concedida pela ISC2 (International Info System Security Certification Consortium) ou concedida pelos representantes e/ou parcerias oficiais da ISC2 no Brasil ou no exterior. O profissional acima indicado deverá integrar quadro técnico da empresa, na data de apresentação da proposta, comprovado por meio das seguintes formas abaixo indicadas:

12.4.1. mediante contrato social (no caso de sócio); ou

12.4.2. registro na carteira profissional, ficha de empregado ou contrato de trabalho; ou

12.4.3. contrato de prestação de serviços, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços quando da assinatura do contrato entre a Licitante e a EMASA.

12.5. A EMASA reserva-se ao direito, caso julgue necessário, de realizar diligências nos documentos acima indicados, a fim de comprovar a execução, o escopo dos serviços fornecidos e a veracidade das informações prestadas.

12.6. Considerando a especificidade do serviço a ser oferecido na contratação em tela, se faz necessário e imprescindível as exigências especificadas neste item.

12.7. O não cumprimento destes requisitos implicará na desclassificação imediata da licitante.

13. DA PROVA DE CONCEITO

13.1. A licitante vencedora após a etapa de lances e de habilitação será submetida à prova de conceito a fim de comprovação de atendimento às exigências técnicas e demais requisitos obrigatórios, contidos no Anexo I deste Termo de Referência.

13.2. A solução apresentada que não atender a 100% (cem por cento) das exigências do caderno de testes Anexo I, da prova de conceito, será considerada inapta, estando, portanto, desclassificada a licitante vencedora, sendo convocada a licitante seguinte na ordem classificatória para realização de prova de conceito e assim sucessivamente até que uma das licitantes participantes apresente solução que atenda plenamente às exigências deste documento;

13.3. A prova de conceito será realizada em sessão aberta a iniciar mediante solicitação do pregoeiro, começando no primeiro dia útil subsequente, caso este prazo coincida com feriado ou final de semana, no horário de 08h às 12h e das 14h às 18h;

13.4. A licitante declarada vencedora na etapa de lances que não comparecer para efetuar a prova de conceito, se recusar por qualquer motivo a efetuar a prova de conceito e/ou não atender aos critérios estabelecidos neste Termo de Referência, inclusive quanto aos requisitos mínimos considerados, será imediatamente considerada inapta para assinatura do contrato, sendo imediatamente desclassificada;

13.5. Serão avaliados todos os itens constantes do roteiro do Anexo I, integrante deste Termo de Referência, respeitado o atendimento de todas as características descritas em cada funcionalidade;

13.6. A realização da prova de conceito e a verificação do cumprimento dos requisitos técnicos obrigatórios previstos no Termo de Referência ficarão a cargo da Comissão Técnica, integrada por empregados designados pela EMASA;

13.7. A prova será executada e julgada pelos membros da Comissão Técnica do CONTRATANTE, com base nos itens constantes Prova de Conceito, Anexo I;

13.8. A comprovação do atendimento às características técnicas especificadas no Termo de Referência dar-se-á por meio da documentação da solução e os datasheet;

13.9. A comprovação das exigências para todos os itens deverá ser realizada em até 05 (cinco) dias úteis, caso necessite deste prazo para conclusão de demonstração;

13.10. Os testes poderão ser executados nas dependências da EMASA obedecendo aos seguintes critérios:

13.11. Toda a infraestrutura necessária à execução da Prova de Conceito deverá ser fornecida pela Licitante, sendo a EMASA responsável apenas pelo fornecimento do espaço físico adequado e

energia elétrica;

13.12. A prova de conceito constituirá da realização do checklist das características/funções mínimas obrigatórias, conforme Prova de Conceito, Anexo I;

13.13. Para a análise do software/solução e da prova de conceito, a sessão será suspensa e retomada somente após a análise acerca da aceitação do software/solução a que se refere, exarando-se a decisão em documento expedido pelo Pregoeiro posteriormente. O acompanhamento da análise de conceito é facultado aos demais licitantes interessados.

13.14. Opcionalmente, serão aceitos testes realizados em ambiente de Nuvem;

13.15. Se, ao final da execução da Prova de Conceito, ficar comprovado o cumprimento de todos os requisitos, a Comissão Técnica emitirá Termo de Verificação, com vistas à aceitação da proposta da Licitante.

14. LOCAL DE PRESTAÇÃO DOS SERVIÇOS ESTABELECIMENTOS DA CONTRATADA E ORDENS DE SERVIÇOS

14.1. Os serviços/treinamentos serão em Balneário Camboriú e Camboriú, nas dependências das unidades da CONTRATANTE, e o atendimento das chamadas técnicas para quaisquer dos serviços contratados deverão ocorrer no prazo máximo de 8 (oito) horas a contar do envio da solicitação, que poderá ser via e-mail, telefone ou sistema de help desk, com o comparecimento do técnico nas dependências da CONTRATANTE. Não considerar sábados, domingos e feriados.

14.2. Todo e qualquer serviço somente será executado pela CONTRATADA mediante uma Ordem de Serviço (O.S.), autorizada por representante do Departamento de Tecnologia da Informação (Gestor do Contrato).

14.3. As Ordens de Serviço serão consideradas como adendos ao Contrato e deverão descrever os serviços de forma detalhada, contemplando a identificação do tipo de serviço, a complexidade, os prazos, os requisitos de qualidade, e o responsável pelo atesto na EMASA.

15. DA FISCALIZAÇÃO:

15.1. Durante a vigência do Contrato, a execução dos serviços será acompanhada e fiscalizada por servidor especialmente designado, o qual assumirá a função de Fiscal de Contrato, nos termos do artigo 67 da Lei 8.666/93;

15.2. A fiscalização deste contrato será realizada pelo SR. COMISSÃO DE RECEBIMENTO DE BENS E SERVIÇOS-, e-mail comissao.materiais@emasa.com.br, fone 47 3261 0000.

15.3. O(s) fiscal(ais) do Contrato anotará(ão) em registro próprio, todas as ocorrências relacionadas com a execução dos serviços contratados, determinando o que for necessário à regularização das faltas ou defeitos observados;

15.4. A omissão, total ou parcial, da fiscalização não eximirá o fornecedor da integral

responsabilidade pelos encargos ou serviços que são de sua competência;

15.5. Ao tomarem conhecimento de qualquer irregularidade ou inadimplência por parte da contratada, os titulares da fiscalização deverão, de imediato, comunicar por escrito ao órgão de administração do contratante, que tomará as providências para que se apliquem as sanções previstas na lei, no Edital e neste Termo de Referência, sob pena de responsabilidade solidária pelos danos causados por sua omissão.

16. REQUISITOS DE SIGILO E SEGURANÇA DA INFORMAÇÃO

16.1. A CONTRATADA deverá obedecer aos critérios, padrões, normas e procedimentos operacionais de mercado e de acordo com as boas práticas;

16.2. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato devendo orientar seus empregados nesse sentido;

16.3. Não transferir a outrem – entidades, fabricantes, técnicos, subempreiteiros – no todo ou em parte, a responsabilidade sobre o objeto do presente contrato sem prévia e expressa anuência por escrito da CONTRATANTE;

16.4. Manter, em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à política de segurança adotada pela CONTRATANTE;

16.5. Executar todos os testes de segurança necessários e definidos na legislação pertinente, quando couber.

17. OBRIGAÇÕES DA CONTRATADA:

17.1. Fica obrigada durante o prazo de validade técnica das respectivas versões, assegurar aos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento da solução, consideradas as suas especificações;

17.2. Quaisquer despesas de transporte, alimentação, hospedagem e outras, decorrentes do contrato, serão de responsabilidade da empresa CONTRATADA. Os eventos ordinários deverão ser precedidos de solicitação por parte da EMASA com prazo mínimo de 24 horas, já os eventos extraordinários, definidos pela EMASA, deverão ter atendimento conforme estabelecido neste Termo de Referência;

17.3. Os técnicos alocados deverão estar aptos para participação de reuniões e treinamentos na região por videoconferência ou pessoalmente, quando for de entendimento entre as partes e dependendo da definição de local;

17.4. Informar à EMASA, para efeito de controle de acesso às suas dependências, o nome, CPF e no número da carteira de identidade dos colaboradores disponibilizados para a prestação de

serviços;

17.5. A empresa vencedora responsabilizar-se-á pela manutenção do sigilo sobre os dados e informações contidas em quaisquer documentos ou mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, reter, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela EMASA a tais documentos. Desta forma, aceita, declara que conhece e obriga-se a cumprir toda a legislação referente às normas e orientações expedidas pela EMASA;

17.6. Prover toda a infraestrutura necessária para hospedar sua solução em um regime de missão crítica, atendendo com uma taxa de disponibilidade mínima de 99% ao ano;

17.7. Deixar disponibilizado acesso ao sistema contratado e dados mesmo após encerramento do contrato por no mínimo após 6 (seis) meses apenas para consulta sem ônus a contratante;

17.8. Fornecer imediatamente assim que solicitado pela EMASA os dados armazenados nos bancos de dados aos quais são pertencentes, ou seja, a base de dados junto com seu dicionário de dados será, em qualquer tempo, de propriedade exclusiva da Autarquia;

17.9. A CONTRATADA não poderá divulgar quaisquer serviços e/ou produtos dela mesma ou de outras aos servidores e/ou canais de comunicação da EMASA, sejam estas divulgações através de sistemas contratados, e-mail, SMS, folders, cartazes, entre outros meios sem que sejam autorizados de maneira expressa pela Diretoria da EMASA;

17.10. É dever da empresa que toda a informação, tem que ser armazenada, com cópias devidamente salvaguardas atendendo à todas exigências da Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), Lei nº 13.709/2018.

17.11. Integrações automáticas de acordo com o SIAFIC, quando e se houverem:

17.11.1. As integrações devem ser diárias, de maneira automatizada e sem intermediários ainda deverão obedecer aos padrões mínimos de qualidade exigidos pelo Decreto Federal nº 10.540, de 05 de Novembro de 2020, que institui o Sistema Único e Integrado de Execução Orçamentária, Administração Financeira e Controle – SIAFIC, e suas alterações posteriores, considerando o sistema específico da contabilidade implantado atualmente na autarquia, e também, caso este venha a ser trocado, que essa adequação seja efetuada sem custos adicionais ao município;

17.12. A contratada deverá atender toda a legislação vigente e suas atualizações determinadas sejam elas demandadas por Órgãos Federal, Estadual e Municipal assim como Agências Reguladoras vinculadas e demandas solicitadas pela contratante;

17.12.1. Quando constatado que o não atendimento a estas determinações, por parte da contratada, ocasionou a geração de multa para a contratante, esta multa será imputada à contratada, por não cumprimento da demanda, sem nenhum ônus para a contratante.

17.12.2. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC

sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração;

17.12.3. Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;

17.12.4. Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

17.12.5. Conduzir os trabalhos com estrita observância às normas da legislação permanentemente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

17.12.6. O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações;

17.12.7. Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua ulização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

18. OBRIGAÇÕES DO CONTRATANTE:

18.1. Efetuar com pontualidade, os pagamentos à contratada, após o cumprimento das formalidades legais;

18.2. Exercer fiscalização sobre o cumprimento das obrigações pactuadas entre as partes;

18.3. A Prefeitura Municipal através de cada unidade administrativa solicitante designara um representante da Administração para fazer a fiscalização e o acompanhamento do cumprimento deste contrato, devendo este fazer anotações e registros de todas as ocorrências, determinando o que for necessário à regularização dos problemas observados, conforme dispõe o artigo 67 da Lei Federal 8.666/1993.

19. DA VISTORIA TÉCNICA

19.1. É facultado às proponentes a realização de vistoria nos locais de execução dos serviços, a fim de obtenção de subsídios para a adequada elaboração de suas propostas comerciais.

19.2. Como é facultado as proponentes, foi elaborado o Anexo 1 para melhor elaboração da proposta e atendimento ao TR.

19.3. A CONTRATANTE não aceitará quaisquer alegações posteriores relativas a desconhecimento das condições dos locais em que serão prestados os serviços como desculpa para o descumprimento de obrigações contratuais ou de exigências contidas neste termo de referência ou no Edital.

19.4. As licitantes se obrigam a declarar que têm pleno conhecimento das condições necessárias para a prestação dos serviços, objeto da licitação.

19.5. Durante a vistoria técnica, a licitante que encontrar algum aspecto incompatível com os termos do edital deverá comunicar formalmente e tempestivamente à Administração, a fim de que esta possa se manifestar também formalmente a respeito e em tempo hábil.

19.6. O silêncio da licitante importará a sua aceitação total e irrestrita a todos os termos do edital.

19.7. No caso da Realização de Vistoria, o Departamento da EMASA emitirá Declaração de Vistoria, assinada conjuntamente por servidor do Departamento e pelo representante da empresa, atestando que o licitante vistoriou as instalações, tomou conhecimento das condições locais e de todos os elementos técnicos necessários ao cumprimento do objeto da licitação, admitindo-se, consequentemente, como certo, o prévio e total conhecimento da situação.

19.8. Alternativamente, a licitante poderá apresentar declaração de renúncia de vistoria devidamente preenchida e assinada pelo seu representante legal, não sendo aceita alegações posteriores relativas a desconhecimento das condições dos locais do serviço como motivo para o descumprimento de obrigações contratuais ou de exigências contidas neste termo de referência ou no Edital.

19.9. A vistoria poderá ser agendada junto ao Departamento, através do telefone (47) 3261-0000, das 12h00 às 17h00, de segunda a sexta feira, no prédio sede da EMASA.

19.10. A visita técnica poderá ocorrer até a véspera à data fixada para a realização da licitação.

ANEXO I – PROVA DE CONCEITO

1 INTRODUÇÃO

1.1. O objetivo deste Plano de Testes e Avaliação é documentar os processos da POC, juntamente com os critérios, tarefas e responsabilidades necessárias para a conclusão da avaliação.

2 CENÁRIO DE TESTES

Os cenários de testes abaixo contemplam os passos que foram alinhados durantes as reuniões de planejamento com o Cliente para emular as condições de produção das plataformas que serão integradas as soluções de criptografia transparente.

Transparent Encryption

Proteção de dados estruturados e não estruturados;

Proteção de File Servers, Pastas, Arquivos, Dados não Estruturados e arquivos de banco de dados;

Criptografar arquivos de forma transparente aos usuários;

Permitir que usuários acessem seus arquivos e pastas de forma transparente;

Criação de Políticas de acesso e controle;

Proteção de acessos indevidos de usuários Privilegiados (root, administrators);

Registro de Logs para todos os acessos permitidos e não autorizados;

Tokenization Server

Tokenizar/Detokenizar dados com preservação de formato e sem preservação de formato;

Testar o mascaramento de dados;

Testar anonimização.

Cloud Key Manager

Gerar uma chave no CCKM e importar automaticamente para a AWS;

Criptografar um bucket S3;

Tentativa de download do arquivo;

Tentativa de download do arquivo com a chave revogada.

Critérios de sucesso para CTE – validação de resultados

A solução de **criptografia transparente CipherTrust** oferece criptografia de dados em repouso com gerenciamento centralizado de chaves, controle de acesso de usuário privilegiado e registro detalhado de auditoria de acesso a dados que ajudam as organizações a atender aos requisitos de relatórios de conformidade e melhores práticas para proteger dados, onde quer que ele resida.

A solução de **criptografia transparente CipherTrust** consiste em um **Gerenciador de segurança de dados (CM)** e um agente CTE residente em seus hosts, seus hosts protegidos ou servidores.

O **CM** é o componente central da solução de CTE. O CM armazena e gerencia dados chaves de criptografia, políticas de acesso a dados, domínios administrativos e perfis de administrador.

O **agente** se comunica com o CM e implementa as diretivas de segurança em seus sistemas **guardpoint** .

Você pode aplicar o CTE a **Guardpoints** nos servidores locais, na nuvem ou a um híbrido de ambos. ou ambos.

O CTE protege os dados criando **diretivas** que especificam a criptografia de arquivos, o acesso a dados e a auditoria em diretórios específicos em seus hosts protegidos. Esses diretórios são chamados de **guardpoints**. As políticas especificam:

Se os arquivos de repouso são ou não criptografados;

Quem pode acessar arquivos desencriptados e quando;

Qual nível de auditoria de acesso a arquivos é desejado, gerando auditoria mais refinadas.

Dentro da estrutura de pastas que abriga os arquivos do banco de dados (Data File), o diretório será protegido utilizando o agente do CTE (Transparent Encryption) as políticas de acesso serão aplicadas para determinados usuários e processos.

- Usuário Diretor: livre acesso
- Usuário Gerente: acesso restrito – somente leitura;
- Usuário Suporte: (administrador/root): acesso restrito – somente cópia (backup);

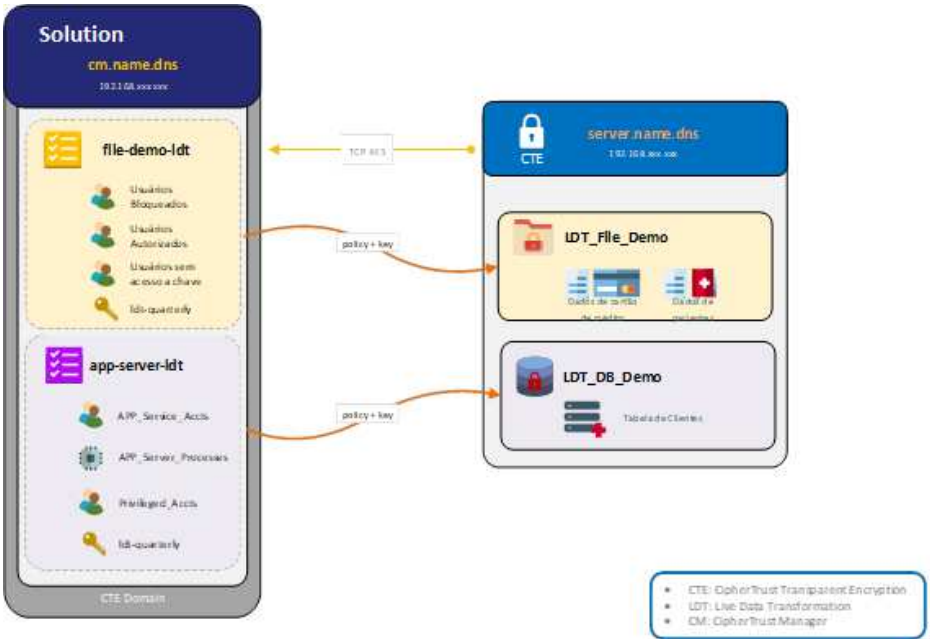


Tabela de testes para o cenário do CTE

Item	Descrição Atividade	Critérios de sucesso	Resultado alcançado
1	Usuário diretor ler/acessar arquivo	Sucesso ao ler/acessar arquivo	

2	Usuário diretor alterar arquivo	Sucesso ao alterar arquivo	
3	Usuário diretor copiar arquivo	Sucesso ao realizar a cópia	
4	Usuário diretor excluir arquivo	Sucesso ao excluir arquivo	
5	Usuário gerente ler/acessar arquivo	Sucesso ao ler/acessar arquivo	
6	Usuário gerente alterar arquivo	Falha ao alterar arquivo	
7	Usuário gerente excluir arquivo	Falha ao excluir arquivo	
8	Usuário suporte ler/acessar arquivo	Falha ao acessar arquivo	
9	Usuário suporte copiar arquivo	Sucesso para cópia de arquivo criptografado	
10	Usuário suporte excluir arquivo	Falha ao excluir arquivo	
11	Acesso aos datafiles para processo do banco de dados no Guardpoint	O processo consegue acessar/ler/alterar informações no banco de dados de forma correta	
11	Log no Gerenciador de Chaves do Usuário suporte tentando renomear, alterar, copiar e deletar arquivo	Registro de log no Gerenciador de Chaves do Usuário suporte das ações realizadas	

Critérios de sucesso para CTS – validação de resultados

A **tokenização** é uma técnica de proteção de dados que substitui dados confidenciais por tokens que normalmente se parecem com os dados originais. Os tokens são inúteis para hackers, administradores desonestos e usuários privilegiados. A tokenização da Thales é aplicada a dados numéricos, como números de cartão de crédito ou de previdência social, e também a dados alfanuméricos, como senha, datas, licenças de motorista, etc.

Políticas de mascaramento de dados também podem ser definidas para fornecer diferentes

visualizações de dados destokenizados com base em permissões de usuário ou grupo..

O CTS fornece **tokens aleatórios** e **tokens criptograficos**. Com tokens aleatórios, a sequência de token não tem relação matemática com os dados originais. Tokens criptograficos são valores que usam algoritmos de **criptografia de preservação de formato (FPE**) para produzir um valor criptografado que retém recursos do conjunto de caracteres original e formatação.

Os usuários abaixo são para descrever os cenários do plano de testes:

- **Diretor**: Usuário com permissões totais, poderá ver o dado totalmente aberto;
- **Gerente**: Usuário irá ver os dados parcialmente aberto;
- **Suporte**: Usuário não terá acesso ao dado e verá completamente mascarado;

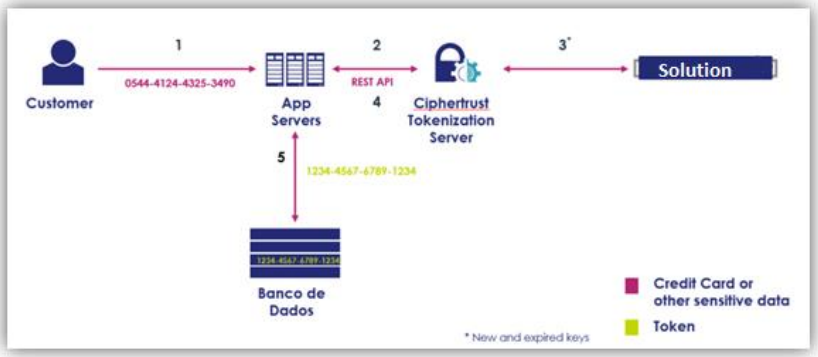


Tabela de testes para o cenário do CTS

Item	Descrição Atividade	Critérios de sucesso	Resultado Alcançado
1	Usuário Diretor solicita a tokenização do dado	Retorno deverá ser um token com o formato preservado	
2	Usuário Diretor solicita dado gravado	Retorno deverá ser o dado totalmente aberto	
3	Usuário Gerente solicita dado gravado	Retorno deve conter dado parcialmente mascarado	
4	Usuário Suporte solicita dado gravado	Retorno deverá trazer o dado totalmente mascarado	

Notas para os testes com CTS:

O usuário “Diretor” que possui nos testes permissão total para a destokenização dos dados e visualização de conteúdo, será utilizado também para Tokenizar as informações;

Uma vez que a informação armazenada no banco de dados não tem valor, isto caracteriza a proteção

dos dados conforme solicitado pela LGPD.

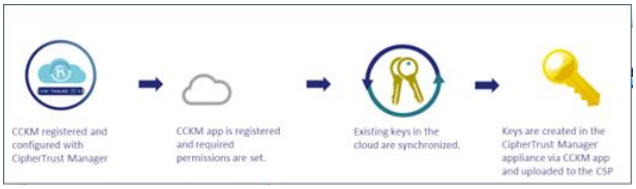
Critérios de sucesso para CCKM – validação de resultados

O CipherTrust Cloud Key Manager (também conhecido como CCKM) centraliza o gerenciamento do ciclo de vida da chave para vários provedores de serviços em nuvem. O CCKM cumpre os mandados de segurança de dados em ambientes de armazenamento em nuvem, mantendo a custódia das chaves de criptografia.

O CipherTrust Cloud Key Manager fornece gerenciamento e armazenamento de chaves e é compatível com os seguintes Cloud Service Providers (CSP):

- Azure
- AWS
- GCP

O CipherTrust Cloud Key Manager é fornecido como parte do dispositivo CipherTrust Manager. Portanto, o CCKM pode ser implantado automaticamente com a implantação do CipherTrust Manager nos ambientes com suporte associados.



Item	Descrição Atividade	Critérios de sucesso	Resultado Alcançado
1	Criar uma chave e fazer o upload automaticamente para a AWS	Retorno deverá ser a cave criada e disponível para uso na AWS	
2	Criptografar um bucket S3 com a chave criada anteriormente	Retorno deverá ser o o bucket criptografado	
3	Fazer o download do arquivo	Retorno deve conter o arquivo descriptografado	
4	Revogar a chave da AWS e fazer o download do arquivo	Retorno deverá ser uma mensagem de acesso negado ao download do arquivo	

ANEXO II

MINUTA

ATA DE REGISTRO DE PREÇOS Nº ____/2022

PREGÃO PRESENCIAL Nº 63/2022 – SRP

Aos XX dias do mês de XXXXX do ano de dois mil e dezenove, a **EMPRESA MUNICIPAL DE ÁGUA E SANEAMENTO DE BALNEÁRIO CAMBORIÚ - EMASA**, inscrita no CNPJ sob o nº 07.854.402/0001-00, neste ato representada pelo Diretor Geral, Sr. Douglas Costa Beber Rocha, inscrito no CPF sob nº. 985.177.830-34, residente e domiciliado na Rua Alvim Bauer, nº 280, Ap. 202, Centro, na cidade de Balneário Camboriú/SC, doravante denominada **EMASA**, considerando o julgamento do **PREGÃO PRESENCIAL PARA REGISTRO DE PREÇOS nº 63/2022** e sua respectiva homologação, conforme processo administrativo nº 98/2022, RESOLVE registrar os preços ofertados pela empresa XXXXXXXXXXXXX, inscrita no CNPJ sob o nº XXXXXXXX, estabelecida à XXXXXXXXXXXXX, CEP XXXXXXXX, e-mail XXXXXXXXXX, telefone (XX) XXXXXX, doravante denominada **FORNECEDORA**, neste ato representada por XXXXXXXXXXXXX, portador do CPF nº XXXXXXXXXX, atendendo as condições previstas no instrumento convocatório e as constantes desta Ata de Registro de Preços, sujeitando-se as partes às normas constantes das Leis nºs 8.666/93 e 10.520/2002 e alterações, do Decreto n° 6.973/2013, Decreto Municipal n° 8.288, de 24 de agosto de 2016 e da Portaria nº 329/2016 e em conformidade com as disposições a seguir.

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. A presente Ata de Registro de Preço – ARP tem por objeto o **REGISTRO DE PREÇOS PARA EVENTUAL CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO PARA PROTEÇÃO INTELIGENTE DE DADOS EM REPOUSO, ESTRUTURADOS E NÃO ESTRUTURADOS, CONTROLE DE ACESSO, VISIBILIDADE E RASTREABILIDADE DE UTILIZAÇÃO DE DADOS EM SERVIDORES DE ARQUIVSOS, BANCO DE DADOS LOCAIS E NUVEM, CUSTÓDIA DE CHAVES CRIPTOGRÁFICAS PARA AMBIENTES EM NUVEM (PÚBLICA, HÍBRIDA OU PRIVADA) COMPOSTA POR SOFTWARES E SERVIÇOS DE GARANTIA E SUPORTE TÉCNICO, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, SERVIÇOS DE TREINAMENTO, SERVIÇOS PARA INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS E SERVIÇOS ESPECIALIZADOS PARA ATENDER ÀS DEMANDAS DA EMASA, CONFORME ESPECIFICAÇÕES TÉCNICAS E DEMAIS CONDIÇÕES CONSTANTES NESTE EDITAL** e vincula-se diretamente aos termos constantes no **Edital de Pregão Presencial nº 63/2026 – Registro de Preços nº 14/2022,** em especial do Anexo I – TERMO DE REFERÊNCIA.

1.2. Este documento registra os preços conforme o que segue:

Lote	ITEM	QTD	Unidade	Descrição da Solução	Métrica	VALOR MÉDIO UNIT - (ANUAL)	VALOR MÉDIO TOTAL (ANUAL)
1	1	4	UN	Fornecimento de agente para proteção de dados para aplicação multiplataforma	Software		
	2	1	UN	Fornecimento de agente para transferência segura de base de dados	Software		
	3	5	UN	Fornecimento de agentes de proteção de dados estruturados multiplataforma	Software		
	4	5	UN	Fornecimento de agentes de proteção de dados não estruturados multiplataforma	Software		
	5	1	UN	Fornecimento de agentes para descoberta e classificação de dados sensíveis - termo de licenciamento por 12 Meses - 15TB	Software		
	6	2	UN	Fornecimento de agentes para gestão de chaves local - 12 meses	Software		
	7	1	UN	Fornecimento de agentes para proteção e custódia de chaves multicloud – termo de licenciamento por 12 meses	Software		
	8	2	UN	Fornecimento de console de gerenciamento de chaves de criptografia em alta disponibilidade	Software		
	9	3	UN	Serviço de Treinamento oficial	Serviço		
	10	12	UN	Serviço de suporte técnico especializado (Helpdesk) – 12 meses	Serviço		
	11	5	UN	Serviço de suporte para agentes de proteção de dados estruturados multiplataforma – 12 meses	Serviço		
	12	5	UN	Serviço de suporte para agentes de proteção de dados não estruturados multiplataforma – 12 meses	Serviço		
	13	4	UN	Serviço de suporte para agentes de proteção de dados para aplicação multiplataforma – 12 meses	Serviço		
	14	2	UN	Serviço de suporte para agentes para gestão de chaves local – 12 meses	Serviço		
	15	2	UN	Serviço de suporte para console de gerenciamento de chaves de criptografia – 12 meses	Serviço		
	16	2	UN	Serviço de Implementação de console de gerenciamento de chaves de criptografia	Serviço		
	17	3000	UST	Serviço sob demanda para Implementação de agentes de criptografia	Serviço		
2	2	12	UN	Serviço de gestão de projetos e documentação - 12 meses	Serviço		
3	3	12	UN	Serviço de análise de risco - 12 meses	Serviço		
4	4	8	UN	Serviço de consultoria para avaliação periódica (HealthCheck)	Serviço		
5	5	12	UN	Serviço de consultoria sob demanda para emissão de relatórios de conformidade com a LGPD - 12 meses	Serviço		
6	6	12	UN	Serviço de diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico	Serviço		
7	7	1	UN	Serviço de suporte de solução para transferência segura de base de dados	Serviço		
					TOTAL		

1.3. **Descrição da solução tecnológica**

1.3.1. A plataforma e/ou ferramental tecnológico deverá atender às seguintes especificações técnicas e requisitos de gestão:

1.3.1.1. A solução ofertada deve reduzir ao máximo a ocorrência de incidentes internos de segurança monitorando a atividade de credenciais com acessos privilegiados (ex. Administradores, root, etc.), bem como impedindo que estes usuários acessem o conteúdo dos dados. Isso tudo, sem que os mesmos percam privilégio para administrar o ambiente de tecnologia;

1.3.1.2. A solução ofertada deve estabelecer o controle de acesso para esse tipo de usuário e identificar atividades suspeitas gerando logs destas atividades;

1.3.1.3. A solução ofertada deve estabelecer um modelo de proteção para informações de tal forma que o dado seja devidamente criptografado no sistema de arquivos. Desta forma, além de impedir a extração não autorizada, mesmo em caso de vazamento acidental dos dados, deverá garantir que os dados não possam ser acessados fora do ambiente gerenciado pela plataforma de segurança, uma vez que não terão a chave de criptografia necessária para acessar a informação;

1.3.1.4. A solução ofertada deve prover mecanismos de prevenção de infecção ou ataques a arquivos por malware, APT, ransomware, ataques gerados por acesso não autorizado, modificações em bibliotecas entre outros, quando estes forem originados de usuários com acesso privilegiado;

1.3.1.5. A solução ofertada deve ser flexível e escalável, adequando-se às necessidades de crescimento da empresa contratante;

1.3.1.6. A solução ofertada precisa permitir a anonimização dos dados pessoais e/ou confidenciais, conforme definido no artigo 12 da Lei Geral de Proteção de Dados Brasileira (LGPD);

1.3.1.7. A solução ofertada deve proteger sistemas de dados estruturado (bancos de dados) e sistemas de dados não estruturado (incluindo arquivos de aplicativos da Microsoft, voz, vídeo e texto em geral) em um ambiente heterogêneo de sistemas operacionais e plataformas de operação;

1.3.2.A solução ofertada deve suportar pelo menos:

1.3.2.1. Sistemas operacionais Microsoft Windows Server, e Linux;

1.3.2.2. Os bancos de dados suportados devem incluir MS-SQL, MySQL e arquivos;

1.3.2.3. Provedores de nuvem suportados devem incluir AWS S3, Azure, Office 365, e IBM Cloud;

1.3.2.4. A solução ofertada deve suportar tudo com console de gerenciamento centralizada para facilitar o processo de administração, controle de acesso, gestão e logs e manutenção da solução de proteção de dados;

1.3.2.5. Soluções baseadas em software livre não serão aceitas.

1.4. **Fornecimento de console de gerenciamento de chaves de criptografia em alta disponibilidade**

1.4.1. A solução deverá prover um console de gerenciamento composta por um conjunto integrado de produtos baseados em uma infraestrutura comum e extensível, com gerenciamento centralizado de políticas e de chaves, reduzindo o esforço de administração e o custo total de propriedade.

1.4.2. O Console de Gerenciamento deve oferecer recursos para proteger e controlar o acesso a dados estruturados e não estruturados hospedados em ambientes físicos e virtuais, ON PREMISES e na NUVEM.

1.4.3. A solução deve prover um console único que permita o gerenciamento centralizado de todos os agentes de criptografia, suas chaves de criptografia, políticas de configuração, publicação e controle de acesso dos dados a serem protegidos.

1.4.4. O console deve possuir certificação FIPS 140-2, Common Criteria, ou outra equivalente, para garantir total segurança das chaves de criptografia.

1.4.5. O console de gerenciamento centralizado deve suportar agentes para as funcionalidades que seguem:

1.4.5.1. Criptografia transparente – para criptografar, controlar o acesso ao dado e oferecer registros de auditoria de acesso aos dados sem impactar nas aplicações, base de dados ou infraestrutura onde quer que os servidores estejam instalados;

1.4.5.2. Integração com SIEM–suportar integração com os sistemas de gerenciamento de logs do mercado, como: Splunk, qRadar, Arcsight, McAfee, LogRhythm e etc;

1.4.5.3. Segurança de container - oferecer criptografia de dados, controle de acesso e registro de acesso ao dado;

1.4.5.4. Gerenciamento de chaves em nuvem múltipla – permitir custódia e controle de dados em ambiente de software como serviço (SaaS), relatório de acesso e eficiência no gerenciamento do ciclo de vida da chave em nuvem com o conceito Traga sua Própria Chave (BYOK);

1.4.5.5. Toquenização e mascaramento de dados - reduzir os custos e o esforço necessários para cumprir com as políticas de segurança e normas regulatórias como o LGPD, dentre outras;

1.4.5.6. Criptografia para aplicações – simplificar o processo de adição de criptografia em aplicações, por meio de Ais baseadas em padrões que potencializam operações criptográficas e de gerenciamento de chaves de alto desempenho.

1.4.6. O console deve ser capaz de ser configurado em alta disponibilidade (HA) com um servidor primário e outro secundário. A configuração de alta disponibilidade deve

permitir a hospedagem dos servidores primário e secundário em datacenters distintos e conectados.

1.4.7. Apoiar a incorporação de vários consoles adicionais para fins de configuração de esquemas de tolerância a falhas multinível.

1.4.8. Os agentes instalados nos servidores devem operar de forma autônoma não causando impacto em caso de perda de comunicação com o console.

1.4.9. Os agentes devem fazer a rotação/mudança de chaves “a quente”, ou seja, sem indisponibilidade nos servidores de dados.

1.4.10. Cada console deve ter a capacidade de suportar o crescimento.

1.4.11. Detalhes da chave de criptografia não devem ser divulgados para usuários do sistema para que o algoritmo de criptografia esteja protegido dos usuários da plataforma. Estes devem ser armazenados de forma segura em um dispositivo virtual dedicado aos serviços de segurança dentro do console.

1.4.12. É desejável que todos os elementos da solução sejam do mesmo fabricante, porém serão aceitas soluções compostas por mais de um fabricante desde que estes fabricantes comprovem interoperabilidade e suporte a solução ofertada.

1.4.13. O console deve possuir capacidade de gerenciar chaves criptográficas padrão KMIP.

1.4.14. Deve ser compatível com API PKCS # 11 e Microsoft Key Extensible Management.

1.4.15. Deve ser capaz de oferecer suporte a certificados digitais (X. 509) PKCS # 7, PKCS # 8 e PKCS # 12, chaves de criptografia simétrica (algoritmos3DES, AES128, AES256, ARIA128 e ARIA256) e assimétrica (algoritmos RSA1024, RSA2048, RSA4096).

1.4.16. Deve ser escalável para oferecer suporte a gerenciamento de agente de vários serviços em uma estrutura de Multitenant e com suporte a configuração de segurança de vários domínios. Para isso, deve possibilitar configurar diferentes chaves criptográficas de acordo com cada área de operação, se necessário.

1.4.17. Quando aplicada a separação de funções, o console deve permitir que o usuário do sistema crie chaves de criptografia, outro usuário pode aplicá-las e outro, que não seja o anterior, consiga monitorar o mesmo durante a aplicação.

1.4.18. Deve requerer autenticação de usuário e senha e, opcionalmente, dois fatores RSA.

1.4.19. Deve ser capaz de configurar cópias de backup de suas configurações automaticamente ou manualmente.

1.4.20. Requerimentos complementares:

1.4.20.1. Suportar usuários múltiplos;

1.4.20.2. Escalabilidade comprovada para mais de 10.000 agentes;

1.4.20.3. Cluster para alta disponibilidade (HÁ);

1.4.20.4. Toolkit e interface de programação;

1.4.20.5. Integração infraestrutura de autenticação existente, com fácil configuração;

1.4.20.6. Suporte para API RESTfull;

1.4.20.7. Autenticação multi-fator;

1.4.20.8. Opções de instalação:

1.4.20.8.1. Sistema virtual com certificação FIPS 140-2 Nível, ou certificação compatível;

1.4.20.8.2. O sistema virtual deve ser compatível com VMware ou Hyper-V.

1.5. **Fornecimento de agentes de proteção de dados estruturados**

1.5.1. Este agente deve fornecer criptografia de banco de dados (dados 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. O agente deverá residir no sistema operacional ou na camada de dispositivo, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela.

1.5.2. O processo de criptografia deve ser executado por agentes que serão instalados nos servidores de banco de dados.

1.5.3. Esses agentes devem oferecer suporte a sistemas operacionais Microsoft, e/ou Linux.

1.5.4. Eles devem ser compatíveis com bancos de dados estruturados e não estruturados, incluindo MS-SQL Server, MySQL.

1.5.5. Deve ser compatível com servidores físicos e versões virtualizadas.

1.5.6. Sua implementação não deve exigir qualquer alteração no banco de dados ou na aplicação.

1.5.7. Estes devem usar os recursos de aceleração disponíveis, como o AES-NI. A implementação destes não deve gerar uma carga incremental, típica em servidores, de mais de 5%.

1.5.8. Além de criptografar o banco de dados, os agentes devem ser capazes de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações estruturadas e não estruturadas (por exemplo: imagens, vídeos, arquivos voz, syslog, etc).

1.5.9. Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso.

1.5.10. As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio.

1.5.11. Essas diretivas devem permitir e serem baseadas em usuário, processo, tipo de arquivo e agendamento.

1.5.12. As políticas devem poder ser aplicadas aos usuários locais, ou igualmente integradas no AD ou no LDAP.

1.5.13. Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com o console de gerenciamento, para poder aplicar processos de criptografia e descriptografia.

1.5.14. Os logs de atividade do usuário devem poder de ser enviados para uma solução de SIEM através de um servidor de syslog ou no formato CEF, em tempo real e nativamente.

1.5.15. A solução deve suportar ambiente em nuvem, tais como AWS, Azure, pelo menos.

1.5.16. A solução deve ter a capacidade de integrar os serviços de gerenciamento de chaves fornecendo serviços de gerenciamento de chaves no local ou na nuvem, para aplicações como Salesforce.com.

1.5.17. Registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos.

1.5.18. Possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados.

1.5.19. Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não criptografado.

1.5.20. Requerimentos complementares:

1.5.20.1. Compatibilidade com os sistemas operacionais:

- Windows Server: 2008, 2012 e posteriores.
- Windows: 7; 8,1, 10 e posteriores.
- Linux: RedHat; CentOS, Ubuntu e Debian.

1.5.20.2. Permitir criptografia para múltiplos fabricantes de banco de dados, tais como:

- MySQL (Windows, Linux);
- MS SQL (Windows).

1.6. **Fornecimento de agente para transferência segura de base de dados**

1.6.1. Este agente deve permitir o mascaramento dos dados sensíveis para permitir o compartilhamento seguro com terceiros, ambientes de teste, ambientes de desenvolvimento e outros casos de uso aplicáveis.

1.6.2. O funcionamento deve ser baseado em tabela e/ou coluna. Informa-se o que deverá ser mascarado no novo banco de dados de destino. Com isso, dados não identificados podem ser compartilhados.

1.6.3. A solução de ser customizável e de alta performance.

1.6.4. A solução deve suportar, pelo menos, as operações de criptografia / tokenização e descriptografia / destokenização de tabelas e / ou colunas.

1.6.5. A solução deve ser transparente para a aplicação ou banco de dados com acesso via conexão ODBC. Ou seja, não deve requerer alterações ou instalações adicionais no servidor de banco de dados.

1.6.6. A solução deve suportar, pelo menos, arquivo CSV, Microsoft SQL Server, MySQL.

1.6.7. A solução deve permitir replicação de arquivo para arquivo, banco de dados para banco de dados, arquivo para banco de dados e banco de dados para arquivo.

1.6.8. Pelo menos os seguintes modelos devem ser suportados: Standard AES Encryption, Batch random Tokenization e Batch FPE FF3/FF1.

1.7. **Fornecimento de agentes de proteção de dados não estruturados multiplataforma**

1.7.1. Este agente deve fornecer criptografia de servidor de arquivo (dado não estruturado) 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. O agente deverá residir no sistema operacional ou na camada de dispositivo, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela.

1.7.2. O processo de criptografia deve ser executado por agentes que deverão ser instalados nos servidores de arquivos.

1.7.3. Os agentes devem oferecer suporte a sistemas operacionais Microsoft e/ou Linux.

1.7.4. Deve ser compatível com servidores físicos e versões virtualizadas.

1.7.5. Sua implementação não deve exigir qualquer alteração no servidor de arquivo ou processo para manuseio do dado pelo usuário final.

1.7.6. Deve ser capaz de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações não estruturadas (por exemplo: imagens, vídeos, arquivos voz, syslog, etc).

1.7.7. Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso.

1.7.8. As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio.

1.7.9. Essas diretivas devem permitir serem baseadas em usuário, processo, tipo de arquivo e agendamento.

1.7.10. As políticas devem ser aplicadas aos usuários locais, ou igualmente integradas no AD ou no LDAP.

1.7.11. Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com o console de gerenciamento para poder aplicar processos de criptografia e descriptografia.

1.7.12. Os logs de atividade do usuário devem ter a capacidade de ser enviado para uma solução de SIEM através de um servidor de syslog ou no formato CEF, em tempo real e nativamente.

1.7.13. A solução deve suportar ambiente em nuvem, tais como AWS, Azure, pelo menos.

1.7.14. Registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos.

1.7.15. Possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados.

1.7.16. Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não criptografado.

1.7.17. Compatibilidade com os sistemas operacionais:

- Windows Server: 2016 e superiores.
- Windows: 10 e superiores.
- Linux: RedHat 7-6; CentOS, Ubuntu e Debian.

1.8. **Fornecimento de agentes de proteção de dados para aplicação multiplataforma**

1.8.1. Este agente deve permitir a toquenização vaultless com o Dynamic Data Masking, para eficientemente Anonimizar dados, incluindo dados pessoais, quer eles residem on premises, ambientes de big data ou a nuvem. Com isso, reduzir o escopo de conformidade substituindo dados confidenciais por um token não-sensível que olha e age como o original. Ou seja, proteção de dados sem a necessidade de alterar bancos de dados. Depois que os dados confidenciais são substituídos pelo token, os sistemas não estão mais sujeitos a conformidade, significando menos esforço para atender regulamentações.

1.8.2. Possuir alto desempenho com baixo impacto na performance da aplicação.

1.8.3. Possuir servidores de token virtual escalável.

1.8.4. Comunicação via TLS autenticado mutuamente.

1.8.5. Interface REST API com chamadas individuais e em lote.

1.8.6. Permitir geração de Tokens Aleatórios.

1.8.7. Compatível com FPE FF1, Tokens FF3.

1.8.8. Permitir Mascaramento Dinâmico ou Estático de Dados.

1.8.9. Gerenciamento de chaves e políticas.

1.8.10. Suporte AD / LDAP.

1.8.11. Suporte a dados numéricos e alfanuméricos.

1.8.12. Permitir a criação de tokens em formatos numéricos, de texto e de data para aplicativos únicos ou múltiplos.

1.8.13. Permitir utilizar grupos de usuários LDAP para decidir quais informações são exibidos para grupos específicos. Por exemplo, operadoras de call center versus gerentes de call center.

1.8.14. Suportar servidor de tokens no formato virtual de sua escolha: OVF, ISO, Microsoft Azure Marketplace ou Amazon AMI.

1.8.15. Restringir o acesso a ativos confidenciais sem alterar os esquemas do banco de dados, sem interrupções.

1.8.16. Proteger dados em trânsito e em repouso.

1.8.17. Mascarar os dados em ambiente de desenvolvimento, teste e terceirizados com acesso ao banco de dados.

1.8.18. DBAs, administradores de sistema, root, e usuários mal-intencionados com acesso direto ao banco, uma vez que os dados que este irão acessar não são dados reais.

1.9. **Fornecimento de agentes para proteção e custódia de chaves multicloud**

1.9.1.A Este agente deve prover o controle de chave pelo próprio cliente permitindo a separação, criação, propriedade, controle e revogação das chaves de criptografia sem a dependência do provedor. Deverá reduzir a complexidade do gerenciamento de chaves, dando ao próprio cliente controle de ciclo de vida de chaves de criptografia com gerenciamento centralizado, visibilidade e rastreabilidade.

1.9.2.Deverá cumprir com os regulamentos de proteção de dados e armazenamento de chaves rigorosos, podendo chegar a FIPS 140-2 Nível 3, ou certificação equivalente.

1.9.3.Prover eficiência com gerenciamento de chave centralizado em ambientes de nuvem híbrida.

1.9.4.Fornecer acesso a cada provedor de nuvem a partir de uma única janela do navegador, incluindo várias contas ou assinaturas.

1.9.5.Rotacionar de forma automática as chaves para cumprir com regulamentações que exigem este serviço de rotação de chave.

1.9.6.Fornecer mecanismos simples, via login federado, para conceder acesso aos dados. Com isso, ser compatível com logins de serviços em nuvem que são autenticados e autorizados pelo provedor de serviços, isto é, nenhum banco de dados de login nem configuração AD ou LDAP é necessário.

1.9.7.Fornecer meios para solicitar a criação de chaves nos provedores de nuvem e fornecer gerenciamento completo do ciclo de vida das mesmas.

1.9.8.Controlar e gerenciar centralizadamente várias nuvens, IaaS e SaaS (Multicloud).

1.9.9. Prover registro (log), rastreabilidade e relatórios de conformidade totalmente independente do provedor de nuvem.

1.9.10. O agente deve suportar, pelo menos, os provedores de nuvem que seguem:

1.9.10.1. Microsoft Azure;

1.9.10.2. Microsoft Office365;

1.9.10.3. Amazon Web Services.

1.10. **Fornecimento de agentes para gestão de chave local**

1.10.1. Ser capaz de centralizar o gerenciamento de chaves de aplicativos de terceiros que usam criptografia nativa, tal como bancos de dados.

1.10.2. O agente deve ter a capacidade de conectar-se com os aplicativos por meio de interfaces padrão e fornecer acesso às funções robustas de gerenciamento de chaves.

1.10.3. Prove simplificação e redução da carga operacional por meio do gerenciamento centralizado de chaves.

1.10.4. Elevar o nível de segurança pela separação das chaves de criptografia das aplicações, banco de dados, storage e etc.

1.10.5. Gerenciar chave utilizando soluções de hardware ou software com certificação FIPS ou equivalente.

1.10.6. Suportar o protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP / PKCS) que é o padrão do setor para troca de chaves de criptografia entre clientes (usuários principais) e um servidor (armazenamento de chaves). A padronização simplifica o gerenciamento de chaves externas.

1.10.7. Garantir a custódia de chaves para, pelo menos:

1.10.7.1. A Oracle TDE;

1.10.7.2. SQL TDE;

1.10.7.3. Nutanix;

1.10.7.4. VMWare;

1.10.7.5. Cisco;

1.10.7.6. Netapp;

1.10.7.7. Certificados;

1.10.7.8. Aplicações desenvolvidas em casa;

1.10.7.9. Outros volumes compatíveis.

1.11. **Fornecimento de agentes para descoberta e classificação de dados sensíveis**

1.11.1. A solução deverá possibilitar a descoberta de dados, em ambiente de dados estruturados e não estruturados, armazenados em diferentes repositórios, tais como:

1.11.1.1. Servidores de Arquivos;

1.11.1.2. Bancos de Dados;

1.11.1.3. Estações de trabalho;

1.11.2. A solução deve permitir, através de interface única, realizar o levantamento e entendimento dos dados existentes, sua localização e riscos associados, permitindo:

1.11.2.1. Atender aos requisitos de privacidade;

1.11.2.2. Obter visibilidade sobre os dados que estão em risco de exposição;

1.11.2.3. Suportar a criação de plano de privacidade e proteção de dados.

1.11.3. A solução ofertada deverá possibilitar, pelo menos, quatro níveis de classificação de dados por padrão:

1.11.3.1. Restrito;

1.11.3.2. Privado;

1.11.3.3. Interno;

1.11.3.4. Público.

1.11.4. A solução deve atribuir pontuações de risco que permitam identificar o nível de sensibilidade dos dados, como arquivos e bancos de dados, agregando os seguintes parâmetros:

1.11.4.1. Nível de proteção;

1.11.4.2. Quantidade de elementos encontrados;

1.11.4.3. Localização;

1.11.4.4. Quantidade de dados confidenciais.

1.11.5. As pontuações de risco devem permitir identificar os dados com maior exposição e permitir priorizar medidas de proteção.

1.11.6. A solução deve suportar os seguintes ambientes:

1.11.6.1. Armazenamento local em Hard Disk e Memória dos computadores;

1.11.6.2. Armazenamentos em rede;

1.11.6.3. Compartilhamento Windows CIS e SMB;

1.11.6.4. Network File System NFS;

1.11.6.5. Bancos de Dados:

1.11.6.6. SQL.

1.11.7. A solução deve suportar os seguintes tipos de arquivos:

1.11.7.1. Banco de Dados:

1.11.7.1.1. Access;

1.11.7.1.2. Dbase;

1.11.7.1.3. SQLite;

1.11.7.1.4. MSSQL MDF & LDF;

1.11.7.2. Arquivos de Imagens:

1.11.7.2.1. BMP;

1.11.7.2.2. FAX;
1.11.7.2.3. GIF;
1.11.7.2.4. JPG;
1.11.7.2.5. PDF;
1.11.7.2.6. PNG;
1.11.7.2.7. TIF.
1.11.7.3. Arquivos compactados:
1.11.7.3.1. bzip2;
1.11.7.3.2. Gzip (todos os tipos);
1.11.7.3.3. TAR;
1.11.7.3.4. Zip (todos os tipos);
1.11.7.4. Microsoft Backup:
1.11.7.4.1. Microsoft Binary / BKF.
1.11.7.5. Microsoft Office: v5, 6, 95, 97, 2000, XP, 2003 e superiores.
1.11.7.5.1. Open Source;
1.11.7.5.2. Star Office;
1.11.7.5.3. Open Office.
1.11.7.6. Padrões abertos:
1.11.7.6.1. PDF;
1.11.7.6.2. HTML;
1.11.7.6.3. CSV;
1.11.7.6.4. TXT.
1.11.7.7. A solução deve classificar os dados como:
1.11.7.7.1. Dado pessoal
1.11.7.7.2. Dados financeiros, com base em modelos integrados ou técnicas de classificação.
1.11.8. Deve possibilitar a identificação de informações padronizadas do Brasil, tais como:
1.11.8.1. Registro Geral (RG);
1.11.8.2. CPF;
1.11.8.3. CNH;
1.11.8.4. Passaporte.
1.11.9. A solução deve permitir a inclusão de modelos de políticas (descoberta e classificação) específicas para LGPD.
1.11.10. A solução deve fornecer relatórios detalhados para demonstrar conformidade com a Lei Geral de Proteção de Dados (LGPD).
1.11.11. A solução deve possibilitar a classificação de dados utilizando:

1.11.11.1. Regex;

1.11.11.2. Patterns;

1.11.11.3. Algoritmos;

1.11.11.4. Contexto.

1.11.12. A solução deve permitir ser implementada “com” ou “sem” agentes instalados.

1.11.13. A solução deve possuir as seguintes características funcionais:

1.11.13.1. Políticas: definir as políticas de privacidade de dados, locais e perfis de varredura e de classificação;

1.11.13.2. Descoberta: localizar dados estruturados e não estruturados, através de toda a organização em ambientes big data, banco de dados e sistema de armazenamento de arquivos;

1.11.13.3. Classificação: classificar dados pessoais e sensíveis, baseado em modelos pré-configurados e técnicas de classificação;

1.11.13.4. Análise de risco: entender a natureza do dado e seus riscos, oferecendo visualizações;

1.11.13.5. Relatórios: gráficos e relatórios de análise de risco, status e alertas durante todo o ciclo de vida do dado.

1.12. **Serviço de treinamento oficial**

1.12.1. O treinamento de capacitação técnica será ministrado para até 8 participantes selecionados pela EMASA, com carga horária mínima de 16 (dezesseis) horas, material oficial do fabricante, e conteúdo necessários a capacitá-los para utilizar o Sistema ofertado.

1.12.2. Deverá ser emitido certificado de participação ao final do curso.

1.12.3. Todo o material didático deve ser repassado de forma impressa e em mídia para os alunos.

1.12.4. Somente serão aceitos materiais oficiais dos fornecedores do Sistema ofertado, e não será permitida a adaptação sobre apostilas/conteúdos de cursos não oficiais.

1.12.5. Os instrutores deverão possuir experiência em didática, além de possuir certificação comprovada na área de segurança, em pelo menos uma das seguintes certificações:

1.12.5.1. ISC2 CSSLP - Certified Secure Software Lifecycle Professional (ISO/IEC 17024);

1.12.5.2. ISC2 CISSP – Certified Information System Security Professional;

1.12.5.3. ISC2 ISSAP – Information System Security Architect Professional;

1.12.5.4. CISM – Certified Information Security Manager;

1.12.5.5. CompTIA Security+: Competency in system security, network infrastructure, access control and organizational security;

1.12.5.6. O treinamento deverá ocorrer nas dependências da CONTRATANTE, ou local por ela indicado na capital do estado, ficando responsável por montar o ambiente adequado para realização do mesmo, isto é, todo o espaço necessário assim como toda infraestrutura computacional e de rede necessária. Caberá à CONTRATADA instalar a solução ou possibilitar o acesso ao Sistema no ambiente de treinamento

1.12.5.7. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento e hospedagem, a confecção e distribuição dos originais do material didático e a emissão de certificados para os profissionais treinados.

1.13. **Serviço de consultoria para avaliação periódica (healthcheck).**

1.13.1. O Serviço deverá rever a implementação existente, validando as suas políticas de operação e proteção. Estes elementos serão avaliados contra as melhores práticas de mercado e as políticas específicas do cliente. Todos os procedimentos operacionais, e configurações deverão ser avaliados e documentados para garantir a estabilidade de integridade e tolerância a falhas.

1.13.2. O Serviço deverá contemplar toda a solução implementada desde as consoles até os agentes de proteção de dados.

1.13.3. Deverá ser executado mediante emissão de ordens de serviço.

1.13.4. Deverá ser executado periodicamente de não excedendo o intervalo de dois meses entre as execuções.

1.13.5. O Serviço deverá ser executado nas dependências do cliente, prioritariamente, em horário comercial. Caso o CLIENTE julgue necessário poderá ser agendada uma janela de manutenção fora do horário comercial sem custos adicionais para a contratante.

1.13.6. As Seguintes atividades deverão ser cobertas pelo serviço:

1.13.6.1. Verificar a configuração da solução, versão instalada e os requisitos de atualização, provendo relatório de impacto e orientação de planejamento para atualização;

1.13.6.2. Verificar a configuração de alta disponibilidade e status de replicação;

1.13.6.3. Verificar os procedimentos para fail-over;

1.13.6.4. Verificar os procedimentos de backup e restauração da plataforma, e as configurações do custodiante da chave;

1.13.6.5. Verificar as configurações de contas de administradores e domínios em relação aos requisitos de segurança;

1.13.6.6. Verificar os níveis e configurações de log atuais, a integração com quaisquer ferramentas SIEM e fornecer qualquer orientação sobre melhorias;

1.13.6.7. Verificar se as melhores práticas para backup automático e chaves estão implementadas e documentadas;

1.13.6.8. Identificar quaisquer políticas atualmente no modo de aprendizagem e o impacto potencial de permanecer nesse estado;

1.13.6.9. Avaliar e verificar os procedimentos gerais de implantação para criar e atualizar políticas e verificar a eficácia geral das políticas;

1.13.6.10. Analisar as configurações de log da solução e fazer as recomendações para eliminar mensagens de log desnecessárias e reduzir o número de logs que a solução precisa processar;

1.13.6.11. Demonstrar e executar relatórios que podem ser usados para verificar os resultados;

1.13.6.12. Revisar os procedimentos de atualização dos agentes de proteção instalados, como políticas de criptografia, configuração de hosts e instalação dos agentes;

1.13.6.13. Revisar os procedimentos operacionais existentes ou procedimentos de implantação de melhores práticas definidos e fazer recomendações e alterações conforme necessário;

1.13.6.14. Emitir relatório de status de saúde geral (HealthCheck) do ambiente contemplando, no mínimo, todos os itens de revisão e verificação;

1.13.6.15. Ao término da execução dos serviços de “HealthCheck” os relatórios deverão serão apresentados à contratada em mídia eletrônica para emissão do termo de aceite da ordem de serviço.

1.14. **Serviço de consultoria sob demanda para emissão de relatórios de conformidade com a LGPD**

1.14.1. O Serviço deverá realizar uma varredura no ambiente protegido pela solução identificando, neste ambiente, todos os pontos de não-conformidade com a LGPD.

1.14.2. O Serviço deverá contemplar toda a solução implementada desde os consoles até os agentes de proteção de dados.

1.14.3. O Serviço deverá ser executado nas dependências do cliente, prioritariamente, em horário comercial. Caso o CLIENTE julgue necessário poderá ser agendada uma janela de manutenção fora do horário comercial sem custos adicionais para a contratante.

1.14.4. As seguintes atividades deverão ser cobertas pelo serviço:

1.14.4.1. Verificar a configuração do agente de descoberta e classificação de dados, versão instalada e os requisitos de atualização, provendo relatório de impacto e orientação de planejamento para atualização;

1.14.4.2. Verificar as configurações de classificação de dados, fazendo as recomendações de melhorias;

1.14.4.3. Verificar a programação de varredura implementada, comparando com as políticas de segurança da contratante;

1.14.4.4. Verificar os logs das últimas varreduras identificando ocorrências de falhas e gerando recomendações para correções;

1.14.4.5. Avaliar as configurações de classificação de dados pessoais / sensíveis de acordo com a LGPD e suas atualizações, quando ocorrerem;

1.14.4.6. Realizar a varredura em todo ambiente atendido pela solução de proteção;

1.14.4.7. Gerar relatório de riscos e painéis gráficos;

1.14.4.8. Gerar relatório de conformidade com a LGPD;

1.14.4.9. Gerar recomendações de correção;

1.14.4.10. Emitir relatório consolidado da varredura com a evidência de todas as atividades realizadas, Painel de conformidade e lista de recomendações.

1.14.5. Ao término da execução dos serviços de “Consultoria sob demanda para emissão de relatórios de conformidade com a LGPD” o (s) relatório (s) deverão ser apresentados à contratada em mídia eletrônica para emissão do termo de aceite da ordem de serviço.

1.15. **Serviço de gestão de projetos e documentação**

1.15.1. Resumo do Projeto, Apresentação, Objetivos, Benefícios, Responsabilidades, Recomendações, Premissas e Restrições;

1.15.2. Gerenciamento do escopo, declaração do escopo, plano de entrega, regras mudanças de escopo.

1.15.3. Gerenciamento do Cronograma e prazos do projeto, bem como gestão dos recursos a serem utilizados.

1.15.4. Gestão de Recursos Humanos alocados no projeto, definição comitê projeto.

1.15.5. Responsabilidades do Comitê do Projeto.

1.15.6. Gerenciamento de Riscos do Projeto e mitigação dos mesmos.

1.15.7. Gerenciamento da Qualidade, métricas e metas de qualidade, lista de verificação de qualidades, documentação de entregas.

1.15.8. Matriz de obrigatoriedade de documentos e artefatos a serem disponibilizados.

1.15.9. Gerenciamento das Comunicações e documentação dos projetos**.**

1.15.10. Diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico.

1.15.11. <u>Detalhamento do Plano de Projeto</u>

1.15.11.1. A CONTRATADA deverá designar um profissional responsável pela gestão do projeto sendo esse o único ponto de contato com a CONTRATANTE;

1.15.11.2. Após a assinatura do contrato, com prazo máximo de 5 (cinco) dias úteis, a CONTRATADA deverá informar o nome, telefone e e-mail do Gerente de Projetos e agendar a data da reunião inicial de projeto (Kick-off meeting);

1.15.11.3. A reunião inicial de projeto deverá seguir a seguinte pauta:

1.15.11.4. Apresentação das equipes CONTRATADA e CONTRATANTE;

1.15.11.5. Apresentação do Detalhamento do Plano de Projeto – Projeto Executivo.

1.15.11.6. Aprovação do Plano do Projeto, após essa etapa iniciar a execução do projeto conforme o plano do projeto – Projeto Executivo.

1.15.12. Detalhamento do plano do Projeto Executivo – Gestão de Projetos

1.15.12.1. Resumo do Projeto, Apresentação, Objetivos, Benefícios, Responsabilidades, Recomendações, Premissas e Restrições;

1.15.12.2. Gerenciamento do escopo, declaração do escopo, plano de entrega, regras mudanças de escopo.

1.15.12.3. Gerenciamento do Cronograma e prazos do projeto, bem como gestão dos recursos a serem utilizados.

1.15.12.4. Estabelecimento de cronograma executivo;

1.15.13. Gestão de Recursos Humanos alocados no projeto, definição comitê projeto:

1.15.13.1. Estabelecimento da lista de contatos e funções definindo claramente;

1.15.13.2. Responsáveis técnicos por cada equipe, profissionais responsáveis pelas definições técnicas do projeto;

1.15.13.3. Executivos de cada equipe, profissionais responsáveis pelos aspectos operacionais, jurídicos e financeiros do projeto;

1.15.13.4. Analistas de cada equipe, profissionais envolvidos nas diversas atividades de projeto;

1.15.14. Responsabilidades do Comitê do Projeto

1.15.14.1. Estabelecimento da matriz de relacionamentos;

1.15.14.2. Estabelecimento da matriz de responsabilidades identificando quem executa, quem precisa ser informado, quem avalia, quem aprova e quem aceita formalmente o resultado em nome da CONTRATANTE;

1.15.14.3. Gerenciamento de Riscos do Projeto e mitigação dos mesmos.

1.15.14.4. Gerenciamento da Qualidade, métricas e metas de qualidade, lista de verificação de qualidades, documentação de entregas.

1.15.14.5. Matriz de obrigatoriedade de documentos e artefatos a serem disponibilizados.

1.15.14.6. Gerenciamento das Comunicações e documentação dos projetos.

1.15.14.7. Estabelecimento do plano de comunicação entre as equipes de forma que todos estejam atualizados em relação às diversas atividades de projeto;

1.15.14.8. Estabelecimento do formato e dos meios de troca de informações entre as equipes da CONTRATADA e da CONTRATANTE.

1.15.14.9. Definição da agenda das reuniões de acompanhamento de projeto.

1.16. **Serviço de suporte técnico especializado (help desk)**

1.16.1. A CONTRATADA deverá possuir um processo de Help-Desk:

1.16.1.1. Nível 1

1.16.1.1.1. Realizar triagem para correta identificação de problemas;

1.16.1.1.2. Prover atendimento via telefone, web, e-mail, chat e acesso remoto à equipamentos (quando disponível);

1.16.1.1.3. Elaborar relatórios técnicos específicos;

1.16.1.1.4. Solucionar dúvidas referentes ao comportamento, comandos, facilidades e características;

1.16.1.1.5. Esclarecer dúvidas sobre mensagens de erro**;**

1.16.1.1.6. Prestar Suporte técnico durante as mudanças;

1.16.1.2. Nível 2

1.16.1.2.1. Prover atendimento especializado para ocorrências complexas;

1.16.1.2.2. Solucionar problemas analisando a causa raiz e propondo planos de ações para evitá-los no futuro;

1.16.1.2.3. Prover informações e recomendações para melhoria dos serviços;

1.16.1.2.4. Prover informações e recomendações para melhoria dos serviços;

1.16.1.2.5. Os profissionais da CONTRATADA executará todas as configurações e customizações necessárias para o pleno funcionamento do ambiente, proporcionando as condições para transferência de know-how;

1.16.1.2.6. Esse serviço deverá ser realizado de forma presencial para assegurar que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos em regime 8 x 5 em horário comercial (08:00 às 18:00);

1.16.1.2.7. A qualidade dos serviços deverá ser assegurada através de processos consolidados e da sólida formação, capacitação e experiência dos profissionais responsáveis pelas atividades;

1.16.1.2.8. OS profissionais da CONTRATADA deverão execução os processos customização de configurações e mudanças, seja em decorrência de alarmes e processos e também por solicitação da CONTRATANTE;

1.16.1.2.9. Os profissionais da CONTRATADA deverão executar as atividades operacionais, utilizando os procedimentos estabelecidos para cada rotina;

1.16.1.2.10. Os profissionais da CONTRATADA deverão executar as atividades de manutenção corretiva, utilizando os procedimentos que permitam maior eficiência e eficácia na solução de falhas;

1.16.1.2.11. Os profissionais da CONTRATADA deverão executar as atividades de manutenção preventiva, rotinas de testes, análises e medidas, utilizando os procedimentos que assegurem mínima interferência na operação e máxima disponibilidade da plataforma;

1.16.1.2.12. Os profissionais da CONTRATADA deverão elaborar procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário;

1.16.1.2.13. As customizações e regras das diversas plataformas serão executadas mediantes chamados específicos obedecendo o SLA acordado;

1.16.1.2.14. Os profissionais da CONTRATADA deverão elaborar relatórios de atividades detalhando os procedimentos realizados e eventuais ajustes, se necessário;

1.16.1.2.15. A CONTRATADA deverá prestar o apoio -técnico para campanhas de segurança para usuários finais, em conjunto com as áreas internas da CONTRATANTE, em especial para as áreas de Tecnologia da Informação e Recursos Humanos, para esclarecimento de usuários sobre os riscos e sobre as boas práticas de segurança digital;

1.16.1.2.16. A CONTRATADA deverá disponibilizar informações técnicas para preparação de material de palestras e informativos, bem como as métricas obtidas através da própria plataforma para ilustração dos principais riscos detectados e mitigados;

1.16.1.2.17. Os profissionais da CONTRATADA deverão promover a manutenção de *appliances* e equipamentos dedicados fornecidos pela CONTRATADA.

1.17. **Serviço de análise de risco – SAR**

1.17.1. Planejamento do gerenciamento de risco;

1.17.2. Identificação dos riscos;

1.17.3. Realização de análise quantitativa (Probabilidade);

1.17.4. Realização da análise Qualitativa (impacto);

1.17.5. Planejar resposta aos riscos;

1.17.6. Controlar os riscos;

1.17.7. Fazer levantamento de ameaças, coletando informações acerca dos seus processos de tecnologia buscando pelas principais ameaças que possam ser claramente identificadas:

1.17.7.1. Perda de dados;

1.17.7.2. Incêndio em data center;

1.17.7.3. Software desatualizados;

1.17.7.4. Sistemas fora do ar;

1.17.7.5. Colaboradores sem treinamento;

1.17.7.6. Excesso de usuários privilegiados;

1.17.7.7. Sistemas operacionais desatualizados;

1.17.7.8. Criação de matriz de risco formada por dois eixos: a probabilidade da ocorrência do risco e o impacto que ele trará caso ocorra;

1.17.7.9. Eixo da probabilidade:

1.17.7.9.1. Quase certo: é praticamente impossível evitar que o risco aconteça, por isso vale a pena pensar em ações de mitigação do impacto do risco depois dele ocorrer;

1.17.7.9.2. alta: a chance de o risco ocorrer é grande e frequentemente ele ocorre de fato;

1.17.7.9.3. média: probabilidade ocasional de acontecimentos do risco. Ainda vale a pena planejar desdobramentos, mas não com tanta preocupação como nos casos anteriores;

1.17.7.9.4. baixa: pouca chance de acontecer algum problema advindo desse risco;

1.17.7.9.5. Rara: É bastante improvável que o risco aconteça, só vale a pena se preocupar em casos de impacto grave ou gravíssimo para o seu projeto.

1.17.7.10. Eixo do impacto:

1.17.7.10.1. Gravíssimo: pode fazer com que o projeto seja cancelado ou que o dano ocasionado por ele seja irreversível;

1.17.7.10.2. Grave: compromete de forma acentuada o resultado do projeto, ocasionando atraso ou insatisfação do cliente;

1.17.7.10.3. médio: perda momentânea ao longo do projeto que pode ser corrigida, mas com o impacto no escopo ou no prazo;

1.17.7.10.4. Leve: desvio quase imperceptível dos objetos do projeto ser facilmente corrigido;

1.17.7.10.5. Sem impacto: não gera nenhum tipo de problema perceptível para o projeto, por isso pode ser ignorado em 99% dos casos. Só dê atenção se esse risco ocorrer quase com certeza e com alta frequência.

1.18. **Serviço de diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico**

1.18.1. Executar diagnóstico de conformidade sobre o ambiente tecnológico do cliente.

1.18.2. Executar levantamento de parque tecnológico, com todas as suas características:

1.18.2.1. Quantidade de servidores de arquivos (dados não estruturados).

1.18.2.1. 1. Qual a versão do sistema operacional (SO) dos Servidores (Windows, Linux e etc).

1.18.2.2. Quantidade de servidores de banco de dados (dados estruturados).

1.18.2.2.1. Qual as versões dos Sistemas operacionais (SO) dos servidores. (Windows, Linux e etc).

1.18.2.2.2. Quais os Banco de dados existentes (Oracle, Mysql, Sql e etc).

1.18.2.3. Executar levantamento por serviço de aplicação que faz chamadas " API REST" Mapeamento de dados sensíveis e seus fluxos de interação entre usuários e dados não estruturados, aplicação/usuários e dados estruturados pré e pós implantação.

1.19. **Serviço de suporte para console de gerenciamento e seus agentes de proteção**

1.19.2.1. Suporte técnico 24x7.

1.19.2.2. Troubleshooting problemas de comunicação com os agentes.

1.19.2.3. Escalação de problemas para as áreas responsáveis de Administração e Operação.

1.19.2.4. Atuação em chamados de problemas e incidentes abertos no Help Desk.

1.19.2.5. Atualização dos chamados.

1.19.2.6. Apoio e esclarecimento de causa raiz do problema.

1.19.2.7. Detalhamento da solução adotada.

1.19.2.8. Documentação de evidências.

1.19.2.9. Confecção de relatórios mensais da saúde e principais eventos do gerenciamento.

1.19.2.10. Caberá a CONTRATANTE, disponibilizar o ambiente tecnológico para que a solução da CONTRATADA seja instalada e configurada;

1.19.2.11. Caberá a CONTRATANTE, disponibilizar os profissionais adequados para fornecer todas as informações necessárias para o desenvolvimento dos serviços;

1.19.2.12. Caberá a CONTRATANTE, informar todos os parâmetros técnicos necessários para que a solução da CONTRATADA seja instalada e configurada;

1.19.2.13. Caberá a CONTRATANTE, disponibilizar ambiente de trabalho adequado para os profissionais da CONTRATADA poderem executar os serviços. Esse ambiente será composto por mesa, cadeira e acesso à rede da CONTRATANTE;

1.19.2.14. A CONTRATADA deverá manter ao longo da vigência do contrato, profissionais qualificados com experiência relacionada às atividades propostas;

1.19.2.15. A contratada, deverá utilizar metodologia e sistema de controle de acesso de forma a possibilitar o rastreamento;

1.19.2.16. A contratada deverá aplicar os conceitos de segurança em telecomunicações, redes e Internet de acordo com as melhores práticas de mercado;

1.19.2.17. A contratada deverá aplicar práticas de Gestão de Segurança e Criptografia de forma a manter o sigilo das informações da CONTRATANTE;

1.19.2.18. A contratada deverá aplicar da melhor forma possível o tratamento da informação que terá acesso mantendo a Confidencialidade, Integridade e Disponibilidade das informações;

1.19.2.19. Os profissionais da contratada deverão prestar atendimento em língua portuguesa;

1.19.2.20. A CONTRATADA deverá prover por meio do mesmo canal de Suporte Técnico Especializado, o atendimento às consultas sobre as falhas de segurança identificadas pela plataforma ou qualquer um dos itens fornecidos, prover auxílio ao tratamento de incidentes encontrados e melhores práticas aplicáveis às medidas recomendadas, além de dirimir dúvidas sobre o ambiente monitorado;

1.19.2.21. O nível de serviço de suporte técnico terá caráter reativo no que diz respeito às solicitações de usuários do Sistema, e preventivo no que diz respeito às atualizações e melhorias em eventuais características ou funcionalidades da solução, e deverá ser prestado remotamente de forma a assegurar os níveis de disponibilidade para manter a solução de segurança ofertada em perfeitas condições de uso;

1.19.2.22. Os serviços de Operação da Plataforma serão prestados pelo período de 12 (doze) meses;

1.19.2.23. A CONTRATANTE, poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência do contrato, para suprir suas necessidades com relação à Plataforma de Segurança;

1.19.2.24. Os serviços de Operação da Plataforma, exceto Service Desk, deverão ser prestados presencialmente nas dependências da

CONTRATANTE seguindo o regime 24x7x365 atendendo aos seguintes requisitos;

1.19.2.25. Local de atendimento: CONTRATANTE;

1.19.2.26. Atendimento presencial: De segunda-feira à sexta-feira exceto feriados;

1.19.2.27. Horário de atendimento presencial: das 8:00 às 18:00;

1.19.2.28. Horário de atendimento remoto: 24 horas por dia;

1.19.2.29. Se necessário, a CONTRATANTE fornecerá credenciais de acesso para os profissionais da CONTRATADA. Essas credenciais serão individuais, não podendo ser compartilhadas entre os profissionais da CONTRATADA. Tais acessos serão auditados;

1.19.2.30. CONTRATANTE deverá emitir o termo de recebimento provisório referente ao serviço de Instalação dos Hardwares, Softwares e Licenças da Plataforma em até 5 (cinco) dias úteis após a entrega do "Relatório de Implementação", e o termo de recebimento definitivo em até IO (dez) dias úteis;

1.19.2.31. Após a assinatura do termo de aceite definitivo fica a CONTRATADA autorizada a emitir a Nota Fiscal relativa aos serviços de implantação;

1.19.2.32. Para fins de comprovação da execução dos serviços mensais de Operação, a CONTRATADA deverá entregar até o quinto dia útil do mês subsequente juntamente com a Nota Fiscal o relatório mensal contendo:

1.19.2.33. Relação dos tickets de atendimento realizados no período;

1.19.2.34. Relação das atividades realizadas no período, contendo, quando couber;

1.19.2.35. Rotinas executadas;

1.19.2.36. Relação das atividades de manutenção preventiva, rotinas de testes, análises e medidas executados;

1.19.2.37. Relação de procedimentos elaborados;

1.19.2.38. Relação de incidentes de segurança que ocorreram no período, contendo:

1.19.2.39. Data e hora da ocorrência;

1.19.2.40. Descrição da ocorrência;

1.19.2.41. Impacto/risco para o negócio;

1.19.2.42. Pessoal notificado.

1.20. **Fornecimento das licenças**

1.20.1 O fornecimento das licenças que compõem a solução deverá ocorrer por intermédio de ordem de fornecimento de bens.

1.20.2. A CONTRATADA terá o prazo de 5 (cinco) dias úteis para realizar a entrega das licenças a partir da data de emissão da ordem de fornecimento de bens.

1.20.3. As licenças deverão ser fornecidas na forma de certificado nomeadas a EMASA, e com os respectivos números de série.

1.20.4. Na ocasião do fornecimento das licenças, deverão ainda ser entregues os aplicativos instaladores (executáveis/binários) acompanhados de documentação técnica em formato digital (manuais de operação) de cada software que compõe a solução.

1.20.5. As licenças serão de 12 meses podendo ser renováveis.

1.21. **Instalação e configuração**

1.21.1. A implantação da solução será realizada por intermédio da abertura de Ordem de Serviço específica.

1.21.2. As seguintes atividades fazem parte de seu escopo:

1.21.3. Elaboração de plano de instalação, contendo todos os requisitos técnicos, etapas, prazos e matriz de responsabilidades;

1.21.4. Instalação da solução todos os módulos que a compõe, no ambiente disponibilizado pela EMASA;

1.21.5. Integração com NOC da EMASA.

1.21.6. Caberá a EMASA disponibilizar o ambiente tecnológico para que a solução da CONTRATADA seja instalada e configurada.

1.21.7. O prazo máximo para a execução do serviço é de 30 (trinta) dias úteis, a contar da data em que a EMASA disponibilizar o ambiente e credenciais de acesso para a execução da instalação e configurações.

1.21.8. Ao término da execução do serviço, a CONTRATADA deverá elaborar um relatório com evidência de todo o processo de instalação, e ceder credenciais de acesso à equipe da EMASA.

1.21.9. O serviço de instalação e configuração da solução foi estimado como atividade de ocorrência única, posto que uma vez concluído, servirá como base para todos os outros serviços que fazem parte do escopo do contrato.

1.21.10. A instalação e configuração da plataforma deverá ser realizada nas dependências da EMASA, em horário comercial.

1.22. Manutenção, suporte técnico e garantia

1.22.1. A CONTRATADA deverá disponibilizar o canal de suporte técnico, através de serviço telefônico, por no mínimo, 8x5 (oito horas por dia, cinco dias por semana), com atendimento, obrigatoriamente em língua portuguesa, falada no Brasil, devendo operar, no mínimo, em dias úteis no horário comercial, das 8h (oito horas) às 18h (dezoito horas), horário de Brasília.

1.22.2. A CONTRATADA deverá fornecer suporte técnico no Brasil, obrigatoriamente em língua portuguesa, falada no Brasil para prestar atendimento e resolver todos os problemas relacionados às possíveis falhas ou interrupções de funcionamento da solução proposta, sempre que solicitado pela EMASA;

1.22.3. A CONTRATADA deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da EMASA. De modo a assegurar alta disponibilidade do canal de suporte técnico para o Sistema fornecido, o registro de chamados deve estar disponível em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados).

1.22.4. Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

1.22.5. A EMASA poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência do contrato, para suprir suas necessidades com relação aos produtos de segurança.

1.22.6. Para efeito de avaliação dos níveis de serviços prestados no suporte técnico, considerar-se-á a contagem de tempo de atendimento apenas para os chamados abertos no curso do período de atendimento, em horário comercial, de modo que os chamados abertos foram deste período serão contabilizados apenas a partir do início do período útil operacional seguinte.

1.22.7. Relatórios sobre a prestação dos serviços:

1.22.8. A contratada fornecerá relatórios mensais sobre a prestação dos serviços, em papel e em arquivo eletrônico, preferencialmente em

formato PDF, com informações analíticas e sintéticas sobre os serviços realizados, incluindo-se chamados abertos e fechados, enfatizando aqueles resolvidos no período.

1.22.9. Constarão dos relatórios dados de todos os chamados ocorridos no período, data e hora de abertura do chamado, data e hora de início do atendimento, data e hora de fechamento do chamado, nome da pessoa que abriu o chamado, nome da pessoa que efetuou o atendimento, descrição do problema e descrição da solução.

1.22.10. Também devem constar dados da reabertura de chamados, quando for o caso, que foram fechados sem serem devidamente resolvidos e que, por esse motivo, necessitaram ser reabertos.

1.22.11. Deverá ainda apresentar relatório para cada solicitação de suporte remoto, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes.

1.22.12. Os atendimentos das ocorrências técnicas devem ser realizados em acordo com os critérios definidos pelos níveis de serviço da tabela abaixo, estando sujeita a CONTRATADA, no caso do descumprimento dos prazos, às sanções especificadas a seguir:

	NÍVEL DE SEVERIDADE DO CHAMADO			
	BAIXA	**MÉDIA**	**ALTA**	**URGENTE**
Descrição do chamado	Problema técnico que gere pouco ou baixo impacto na utilização da solução.	Problema técnico que impeça a utilização parcial de uma funcionalidade, não impedindo por completo seu uso.	Problema técnico que impeça completamente a utilização de uma funcionalidade.	Problema técnico que impeça a utilização da solução em sua totalidade.
Prazo para atendimento da ocorrência	Até 12 horas úteis	Até 8 horas úteis	Até 4 horas úteis	Até 0,5 horas úteis

1.22.13. Sempre que o fabricante da solução disponibilizar versões mais atuais da solução oferecida, a licitante deverá fornecer estas versões e releases dos softwares da solução para a EMASA, sem ônus adicionais, enquanto o contrato estiver vigente.

1.22.14. Entende-se por manutenção corretiva a série de procedimentos destinados ao restabelecimento operacional da

solução com todas suas funcionalidades, motivados pela ocorrência de incidentes na solução e/ou problemas recorrentes na solução, compreendendo, inclusive, atualização de softwares por um substituto de igual ou maior configuração, ajustes, reparos, correções necessárias;

1.22.15. Entende-se por suporte técnico aquele efetuado mediante atendimento telefônico ou remoto, para resolução de problemas e esclarecimentos de dúvidas sobre a configuração e utilização da solução.

1.22.16. Os serviços deverão ser realizados por meio de técnicos especializados, devidamente credenciados para prestar os serviços de garantia e assistência técnica remoto, de forma rápida, eficaz e eficiente, sem quaisquer despesas adicionais para a EMASA, inclusive quanto às ferramentas, equipamentos e demais instrumentos necessários à sua realização.

1.23. Descrição dos serviços especializados

1.23.1. O fornecimento dos serviços especializados objeto deste certame observará o seguinte quantitativo:

Item	Descrição	Unidade	Quantidade
23	SERVIÇOS SOB DEMANDA PRA IMPLEMENTAÇÃO DE AGENTES DE CRIPTOGRAFIA	UST	3.000

1.23.2. Os serviços especializados tratam da operacionalização da gestão de chaves criptográficas, com apoio presencial de pessoal especializado ou remoto caso definido pela EMASA, devendo ser solicitado mediante emissão de ordem de serviço, informando às aplicações que farão parte do escopo do serviço.

1.23.3. Todas as atividades desempenhadas relativas aos serviços especializados deverão ser executadas nas dependências da EMASA, respeitando o horário de funcionamento da EMASA, e com o acompanhamento e ciência dos servidores.

1.23.4. Os serviços especializados serão demandados de acordo com a necessidade da EMASA, de forma proporcional ao número de agentes de criptografia instalados, mensurados através da métrica de UST, considerando que uma hora de trabalho equivale a uma UST.

1.23.5. Dada as diferentes atividades que compõem os serviços especializados, foram definidos três níveis de complexidade que visam garantir o equilíbrio físico-financeiro de sua execução, conforme disposto na tabela abaixo:

Nível de Complexidade	Definição
Normal	Cada hora de trabalho equivale a uma UST.
Média	Cada hora de trabalho equivale a duas UST's
Alta	Cada hora de trabalho equivale a três UST's.

1.23.6. Os serviços especializados deverão ser executados por colaboradores da CONTRATADA, respeitando as normas de segurança da informação da EMASA, executando as atividades observando criteriosamente o escopo definido nas respectivas ordens de serviços.

2. CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DAS PARTES

2.21. Constituem obrigações da EMASA:

a) notificar a CONTRATADA quanto à requisição do material mediante o envio da nota de empenho, a ser repassada via email ou retirada pessoalmente pelo fornecedor;

b) permitir ao pessoal da contratada o acesso ao local da entrega do objeto, desde que observadas as normas de segurança;

c) notificar o fornecedor de qualquer irregularidade encontrada no fornecimento do material;

d) efetuar os pagamentos devidos, observadas as condições estabelecidas nesta Ata;

e) promover ampla pesquisa de mercado, de forma a comprovar que os preços registrados permanecem compatíveis com os praticados no mercado.

Parágrafo único - Esta Ata não obriga a EMASA a firmar contratações com os fornecedores cujos preços tenham sido registrados, podendo ocorrer licitações específicas para aquisição do objeto desta Ata, observada a legislação pertinente, sendo assegurada preferência de fornecimento ao detentor do registro, em igualdade de condições.

2.22. **Constituem obrigações do fornecedor**:

a) assinar esta Ata e retirar a respectiva nota de empenho, no prazo máximo de 5 (cinco) dias úteis, contado da convocação;

c) fornecer o material conforme especificação, marca e preço registrados;

d) entregar as licenças/softwares solicitado no respectivo endereço do órgão participante da presente Ata de Registro de Preços, no prazo máximo de 10 (dez) dias, a contar do recebimento da nota de empenho;

e) Fica obrigada durante o prazo de validade técnica das respectivas versões, assegurar aos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento da solução, consideradas as suas especificações.

f) Quaisquer despesas de transporte, alimentação, hospedagem e outras, decorrentes do contrato, serão de responsabilidade da empresa CONTRATADA. Os eventos ordinários deverão ser precedidos de solicitação por parte da EMASA com prazo mínimo de 24 horas, já os eventos extraordinários, definidos pela EMASA, deverão ter atendimento conforme estabelecido neste Edital.

g) Os técnicos alocados deverão estar aptos para participação de reuniões e treinamentos na região por videoconferência ou pessoalmente, quando for de entendimento entre as partes e dependendo da definição de local.

h) Informar à EMASA, para efeito de controle de acesso às suas dependências, o nome, CPF e no número da carteira de identidade dos colaboradores disponibilizados para a prestação de serviços.

j) A empresa vencedora responsabilizar-se-á pela manutenção do sigilo sobre os dados e informações contidas em quaisquer documentos ou mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, reter, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela EMASA a tais documentos. Desta forma, aceita, declara que conhece e obriga-se a cumprir toda a legislação referente às normas e orientações expedidas pela EMASA.

k) Prover toda a infraestrutura necessária para hospedar sua solução em um regime de missão crítica, atendendo com uma taxa de disponibilidade mínima de 99% ao ano.

l) Deixar disponibilizado acesso ao sistema contratado e dados mesmo após encerramento do contrato por no mínimo após 6 (seis) meses apenas para consulta sem ônus a contratante.

m) Fornecer imediatamente assim que solicitado pela EMASA os dados armazenados nos bancos de dados aos quais são pertencentes, ou seja, a base de dados junto com seu dicionário de dados será, em qualquer tempo, de propriedade exclusiva da Autarquia.

o) A CONTRATADA não poderá divulgar quaisquer serviços e/ou produtos dela mesma ou de outras aos servidores e/ou canais de comunicação da EMASA, sejam estas divulgações através de sistemas contratados, e-mail, SMS, folders, cartazes, entre outros meios sem que sejam autorizados de maneira expressa pela Diretoria da EMASA.

p) É dever da empresa que toda a informação, tem que ser armazenada, com cópias devidamente salvaguardas atendendo à todas exigências da Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), Lei nº 13.709/2018.

q) Integrações automáticas de acordo com o SIAFIC, quando e se houverem:

q.1) As integrações devem ser diárias, de maneira automatizada e sem intermediários ainda deverão obedecer aos padrões mínimos de qualidade exigidos pelo Decreto Federal nº 10.540, de 05 de Novembro de 2020, que institui o Sistema Único e Integrado de Execução Orçamentária,

Administração Financeira e Controle – SIAFIC, e suas alterações posteriores, considerando o sistema específico da contabilidade implantado atualmente na autarquia, e também, caso este venha a ser trocado, que essa adequação seja efetuada sem custos adicionais ao município.

r) A contratada deverá atender toda a legislação vigente e suas atualizações determinadas sejam elas demandadas por Órgãos Federal, Estadual e Municipal assim como Agências Reguladoras vinculadas e demandas solicitadas pela contratante.

r.1) Quando constatado que o não atendimento a estas determinações, por parte da contratada, ocasionou a geração de multa para a contratante, esta multa será imputada à contratada, por não cumprimento da demanda, sem nenhum ônus para a contratante.

r.2) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração.

r.3) Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão.

r.4) Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010.

r.5) Conduzir os trabalhos com estrita observância às normas da legislação permanentemente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

r.6) O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações.

r.7) Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua ulização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

s) Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato devendo orientar seus empregados nesse sentido.

t) Não transferir a outrem – entidades, fabricantes, técnicos, subempreiteiros – no todo ou em parte, a responsabilidade sobre o objeto do presente contrato sem prévia e expressa anuência por escrito da CONTRATANTE.

u) Manter, em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à política de segurança adotada pela CONTRATANTE.

v) Executar todos os testes de segurança necessários e definidos na legislação pertinente, quando couber.

v) Ressarcir os eventuais prejuízos causados aos órgãos gerenciadores e participante(s) e/ou a terceiros, provocados por ineficiência ou irregularidades cometidas na execução das obrigações assumidas.

3. CLÁUSULA TERCEIRA– DA VIGÊNCIA

3.21. A presente Ata de Registro de Preços terá vigência pelo prazo de 12 (doze) meses, iniciando com a data da publicação da mesma, prorrogável na forma do art. 4º, § 2º, do Decreto nº 3.931/01.

4. CLÁUSULA QUARTA – DO GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS

4.21. O gerenciamento deste Instrumento, no aspecto operacional, caberá ao Departamento Requisitante do Registro, competindo-lhe:

4.21.1. Fiscalizar a sua execução, atestar as notas fiscais para efeito de pagamento, bem como tomar as medidas necessárias à solução de quaisquer contratempos e/ou irregularidades que porventura venham a ocorrer.

4.21.2. Comunicar à Comissão de Registro de Preços quaisquer problemas ou eventos não previstos neste Ata ou no Edital que lhe dê origem.

4.21.3. Coordenar as formalidades e fiscalizar o cumprimento das condições ajustadas no edital da licitação e na presente Ata.

4.22. O gerenciamento deste Instrumento, no contratual, caberá à Comissão de Registro de Preços da EMASA, competindo-lhe:

4.22.1. Efetuar controle dos fornecedores, dos preços, dos quantitativos fornecidos e das especificações do material registrado.

4.22.2. Monitorar, periodicamente, os preços do material, de forma a avaliar o mercado, podendo rever os preços registrados, a qualquer tempo, em decorrência da redução dos preços praticados no mercado ou de fato que eleve os custos dos bens registrados.

4.22.3. Notificar o fornecedor registrado via email ou telefone, para retirada da nota de empenho.

4.22.4. É de responsabilidade do Contratado verificar sua caixa de entrada de emails e as publicações oficiais da EMASA.

4.22.5. Observar, durante a vigência da presente ata, que nas contratações sejam mantidas as condições de habilitação e qualificação exigidas na licitação, bem como a compatibilidade com as obrigações assumidas, inclusive, solicitar novas certidões ou documentos vencidos.

4.22.6. Conduzir eventuais procedimentos administrativos de renegociação de preços registrados, para fins de adequação às novas condições de mercado e de aplicação de penalidades.

4.22.6.1. As pesquisas de mercado, atendendo à conveniência e ao interesse público, poderão ser realizadas por entidades especializadas, preferencialmente integrantes da Administração Pública, assim como ser utilizadas pesquisas efetuadas por órgãos públicos.

4.22.6.2. A Comissão de Registro de Preços será responsável pelas pesquisas de preços dos itens registrados, de forma a avaliar os preços a serem contratados, bem como elaborará as estimativas de consumo e os cronogramas de contratação.

5. CLÁUSULA QUINTA - DOS PREÇOS

5.21. Os preços registrados, a especificação do material, o quantitativo, as marcas, as empresas fornecedoras e o nome do representante legal são os constantes da Ata do Pregão Presencial nº 63/2022.

5.22. As despesas decorrentes do objeto desta licitação correrão por conta da seguinte disponibilidade orçamentária: funcional programática 35.001.17.512.1916, Projeto 2.189 – Manutenção das Atividades Administrativas da EMASA.

5.23. A EMASA monitorará, periodicamente, por meio da Comissão de Registro de Preços os preços dos produtos, avaliará o mercado constantemente e poderá rever os preços registrados a qualquer tempo, em decorrência da redução dos preços praticados no mercado ou de fato que eleve os custos dos bens registrados.

5.24. A EMASA convocará o fornecedor para negociar o preço registrado e adequá-lo ao preço de mercado, sempre que verificar que o preço registrado está acima do preço de mercado.

5.25. Em qualquer hipótese os preços decorrentes da revisão não poderão ultrapassar aos praticados no mercado, mantendo-se a diferença percentual apurada entre o

valor originalmente constante da proposta do fornecedor e aquele vigente no mercado à época do registro, mantendo-se a equação econômico-financeira.

5.26. Caso seja frustrada a negociação, o fornecedor será liberado do compromisso assumido.

5.27. Antes do pedido, e caso seja frustrada a negociação, o fornecedor poderá ser liberado do compromisso assumido, caso comprove mediante requerimento fundamentado e apresentação de comprovantes (notas fiscais de aquisição de matérias-primas, lista de preços de fabricantes, etc.), que não pode cumprir as obrigações assumidas, devido ao preço de mercado ter se tornado superior ao preço Não havendo êxito nas negociações com o primeiro colocado, no item, a EMASA poderá convocar os demais fornecedores classificados nas mesmas condições, conforme cadastro de reserva anexo a esta ATA, ou revogar a Ata de Registro de Preços.

5.28. As alterações de preços oriundas da revisão dos mesmos, no caso de desequilíbrio da equação econômico-financeira, serão publicadas trimestralmente no Diário Oficial do Município ou publicação que o substitua.

6. CLÁUSULA SEXTA - DO CANCELAMENTO DO REGISTRO DE PREÇOS

6.21. Os preços registrados na presente Ata de Registro de Preços poderão ser cancelados de pleno direito, conforme a seguir:

6.21.1. Por iniciativa da Administração:

a) quando o fornecedor der causa à rescisão administrativa da nota de empenho decorrente deste Registro de Preços, nas hipóteses previstas nos incisos de I a XII e XVII do art. 78 da Lei 8.666/93;

b) se os preços registrados estiverem superiores aos praticados no mercado.

6.22. Por iniciativa do fornecedor:

a) mediante solicitação escrita, comprovando estar o fornecedor impossibilitado de cumprir os requisitos desta Ata de Registro de Preços;

b) quando comprovada a ocorrência de qualquer das hipóteses contidas no art. 78, incisos XIV, XV e XVI, da Lei nº 8.666/93.

6.23. Ocorrendo cancelamento do preço registrado, o fornecedor será informado por correspondência com aviso de recebimento, a qual será juntada ao processo administrativo da presente Ata.

6.24. No caso de ser ignorado, incerto ou inacessível o endereço do fornecedor, a comunicação será feita por publicação no Diário Oficial do Estado, considerando-se cancelado o preço registrado.

6.25. A solicitação do fornecedor para cancelamento dos preços registrados poderá não ser aceita pelo EMASA, facultando-se a este, neste caso, a aplicação das penalidades previstas nesta Ata.

6.26. Havendo o cancelamento do preço registrado, cessarão todas as atividades do fornecedor relativas ao respectivo registro.

6.27. Caso se abstenha de aplicar a prerrogativa de cancelar esta Ata, o EMASA poderá, a seu exclusivo critério, suspender a sua execução e/ou sustar o pagamento das faturas, até que o fornecedor cumpra integralmente a condição contratual infringida.

7. CLÁUSULA SÉTIMA – DO RECEBIMENTO

7.21. Objeto deste contrato deverá ser entregue na sede administrativa da EMASA, localizada na Quarta Avenida N° 250, Centro, Balneário Camboriú/SC, CEP 88330104.

7.22. As quantidades indicadas no Termo de Referência referem-se à previsão de consumo total no período de vigência da Ata, ficando as entregas condicionadas à emissão da nota de empenho pela EMASA.

7.23. O encaminhamento da nota de empenho será efetuado mediante envio, pelo Departamento responsável da EMASA, de correspondência eletrônica ao endereço eletrônico da contratada constante na proposta de preços.

7.24. No ato de entrega do objeto, a contratada deve apresentar documento fiscal válido correspondente ao fornecimento.

7.25. Somente serão aceitos produtos/materiais novos, não sendo admitida, em hipótese alguma, a entrega de produtos/materiais reutilizados ou recondicionados, nem fora de linha de fabricação.

7.26. Os produtos/materiais deverão ser entregues no prazo e locais indicados no Termo de Referência.

7.27. Os produtos/materiais serão recebidos provisoriamente no ato da entrega, para efeito de posterior verificação da conformidade do item com as especificações constantes do Anexo I e na proposta comercial.

7.28. Os produtos/materiais poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste edital e/ou na proposta comercial, devendo ser substituídos às expensas do fornecedor no prazo de 05 (cinco) dias, contado a partir da data da notificação.

7.28.1. Neste caso serão interrompidos os prazos de recebimento e suspenso o pagamento, até que sanada a situação, quando ocorrerá

um novo recebimento provisório, e o reinício de contagem dos prazos.

7.28.2. Os produtos/materiais rejeitados deverão ser retirados no endereço informado no Anexo I, às custas do fornecedor.

7.28.3. A EMASA não arcará com nenhum ônus advindo da troca de itens rejeitados, nem mesmo enviará produtos/materiais via correio ou por qualquer outra forma.

7.29. Os produtos/materiais serão recebidos definitivamente no prazo de 5 (cinco) dias, contado a partir da data da entrega, após a verificação da qualidade e quantidade do material e consequente aceitação, na forma do art. 73, inciso II e parágrafos, da Lei nº 8.666/93, mediante a lavratura de termo circunstanciado.

7.30. Na hipótese de o termo circunstanciado ou a verificação não serem, respectivamente, lavrado ou procedida dentro dos prazos fixados, reputar-se-ão como realizados, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

7.31. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade do fornecedor por quaisquer danos causados à Administração ou a terceiros, decorrentes da utilização do material fornecido.

7.32. O fornecedor deverá informar, se for o caso, qualquer condição especial para armazenamento e/ou transporte do produto/material fornecido.

8. CLÁUSULA OITAVA – DO PAGAMENTO

8.21. O pagamento será efetuado mensalmente e em até 30 (trinta) dias, mediante protocolo da nota fiscal com toda documentação completa exigida, devidamente aprovada pela respectiva Comissão de Recebimento da EMASA, nas condições da proposta apresentada.

8.22. Todos os pagamentos serão realizados exclusivamente por depósito bancário.

8.23. É CONDIÇÃO INDISPENSÁVEL PARA A EFETUAÇÃO DO PAGAMENTO, A COMPROVAÇÃO, POR PARTE DO CONTRATADO, DA REGULARIDADE COM O INSS E FGTS.

8.24. AS NOTAS FISCAIS DEVERÃO INDICAR O Nº DE SUA NOTA DE EMPENHO E, QUANDO FOR O CASO, O NÚMERO DO CONTRATO.

8.25. O NÃO CUMPRIMENTO DOS ITENS 8.3 E 8.4 CULMINAM NA DEVOLUÇÃO DA NOTA FISCAL.

8.26. Se o contratante não efetuar o pagamento no prazo previsto e tendo o contratado, à época, adimplido integralmente as obrigações avençadas, inclusive o disposto

no subitem 14.2, os valores devidos serão monetariamente atualizados, a partir do dia de seu vencimento e até o dia de sua liquidação, segundo os mesmos critérios adotados para atualização de obrigações tributárias, conforme estabelecido no artigo 117 da Constituição Estadual.

9. CLÁUSULA NONA – DAS SANÇÕES

9.21. O licitante/fornecedor que, convocado dentro do prazo de validade de sua proposta, não assinar a Ata de Registro de Preços, deixar de entregar documentação exigida neste Edital, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta/lance, falhar ou fraudar na execução da Ata/Contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedido de licitar e de contratar com a EMASA e o Município, pelo prazo de até 2 (dois) anos, sem prejuízo das sanções previstas neste Edital e na Ata de Registro de Preços e das demais cominações legais.

9.22. O encaminhamento de Ofício de Notificação poderá ser efetuado pelo Departamento responsável da EMASA por meio de endereço eletrônico, para fins de garantia do direito à ampla defesa em caso de inexecução total ou parcial de quaisquer dos atos dispostos no item precedente.

9.23. Além do envio do email, a EMASA publicará em jornal de circulação local o extrato do Ofício de Notificação.

9.24. É de responsabilidade do Contratado verificar sua caixa de entrada de emails e as publicações oficiais da EMASA.

9.25. Se no decorrer da sessão pública da licitação ou na execução do objeto do presente Edital ficar comprovada a existência de qualquer irregularidade ou ocorrer inadimplemento contratual pelo qual possa ser responsabilizado o licitante/contratado, este poderá sofrer as seguintes penalidades:

a) Advertência por escrito;

b) Multa de 10% (dez por cento), calculada sobre o valor total atualizado da proposta ou lance, na hipótese de desistência injustificada da proposta ou lance após a fase de habilitação;

c) Multa de 10% (dez por cento), calculada sobre o valor total atualizado da Ata de Registro de Preços, na hipótese de recusa injustificada do licitante vencedor em assinar a Ata de Registro de Preços e/ou retirar ou confirmar o recebimento da nota de empenho, no prazo máximo de 5 (cinco) dias úteis, após regularmente convocado, caracterizando inexecução total das obrigações acordadas;

d) Multa de 0,33% (zero vírgula trinta e três por cento) por dia de atraso, incidente sobre o valor total atualizado da contratação, pelo atraso injustificado para o fornecimento/substituição de produtos/materiais, a ser cobrada pelo período máximo de 30 (trinta) dias. A partir do 31º (trigésimo primeiro) dia de atraso, a contratação será anulada e a Ata de Registro de Preços será cancelada;

e) Multa de 5% (cinco por cento) sobre o valor total atualizado da contratação, nos casos de anulação da contratação por culpa da contratada;

f) Multa de até 5% (cinco por cento) sobre o valor total atualizado da contratação quando for constatado o descumprimento de qualquer obrigação ou condição prevista neste Edital e/ou no Termo de Referência, em qualquer hipótese de inexecução total ou parcial, ou qualquer outra irregularidade na execução do objeto, ressalvadas aquelas obrigações para as quais tenham sido fixadas penalidades específicas, aplicada em dobro na reincidência.

9.26. A aplicação das sanções previstas neste Edital não exclui a possibilidade de aplicação de outras, previstas na Lei nº 8.666/93 e no Decreto nº 6.973/13, inclusive a responsabilização do licitante vencedor por eventuais perdas e danos causados à EMASA.

9.27. As multas aplicadas deverão ser recolhidas à EMASA, por meio de depósito em conta corrente, observando-se sua data de vencimento, podendo a Administração cobrá-las judicialmente, com os encargos correspondentes, ou descontá-las dos valores remanescentes de pagamentos à empresa.

10. CLÁUSULA DEZ – DA RESCISÃO

10.21. O inadimplemento de cláusula estabelecida nesta Ata de Registro de Preço, por parte do fornecedor, assegurará à EMASA o direito de rescindi-lo, mediante notificação, com prova de recebimento.

10.22. Além de outras hipóteses expressamente previstas no artigo 78 da Lei 8.666/93, constituem motivos para a rescisão da contratação:

a) atraso injustificado no fornecimento, bem como a sua paralisação sem justa causa e prévia comunicação à EMASA;

b) o cometimento reiterado de falhas comprovadas por meio de registro próprio efetuado pelo representante da EMASA

10.23. Nos casos em que o fornecedor sofrer processos de fusão, cisão ou incorporação, será admitida a continuação desta contratação desde que a execução da presente Ata não seja afetada e que o fornecedor mantenha o fiel cumprimento dos termos deste documento e as condições de habilitação.

10.24. À EMASA é reconhecido o direito de rescisão administrativa, nos termos do artigo 79, inciso I, da Lei nº 8.666/93, aplicando-se, no que couber, as disposições dos parágrafos primeiro e segundo do mesmo artigo, bem como as do artigo 80.

11. CLÁUSULA ONZE – DA PUBLICAÇÃO

11.21. De conformidade com o disposto no parágrafo único do artigo 61, da Lei 8.666/93, a presente Ata de Registro de Preços será publicado na forma de extrato, em jornal de circulação local até o 5º dia útil do mês subsequente.

12. CLÁUSULA DOZE – DAS DISPOSIÇÕES GERAIS

12.21. A EMASA não recebe documentos físicos (notas fiscais, certidões, relatórios, medições, etc). Todo recebimento de documentos se dará através de protocolo eletrônico. Sendo assim, o recebimento de mercadorias somente se efetivará após o pré-agendamento junto ao Setor de Almoxarifado, da Nota Fiscal e certidões devidamente anexadas ao protocolo eletrônico que deve ser aberto no sistema 1DOC. O fornecedor/entregador deverá informar o número do protocolo eletrônico na portaria da EMASA, no momento da entrega, para que sua entrada seja autorizada. A AUSÊNCIA DO DEVIDO PROTOCOLO ELETRÔNICO COM SEUS ANEXOS, IMPLICARÁ NA RECUSA DO RECEBIMENTO!

12.21.1. **As notas fiscais e seus anexos devem ser protocoladas eletronicamente pelo site: https://emasa.1doc.com.br/atendimento**

12.21.2. **Cada protocolo deve conter apenas 01 (uma) nota fiscal.**

12.22. PARA PROTOCOLAR AGENDAMENTO DE ENTREGA DE MATERIAIS, É IMPRESCINDÍVEL ANEXAR:

12.22.1. **Nota fiscal;**

12.22.2. **Certidão Negativa de Débitos Federais;**

12.22.3. **Certificado de Regularidade do FGTS – CRF;**

12.22.4. **Autorização de Uso da nota fiscal eletrônica.**

12.23. PARA PROTOCOLAR NOTA FISCAL DE SERVIÇOS É IMPRESCINDÍVEL ANEXAR:

12.23.1. **Nota fiscal;**

12.23.2. **Relatório dos serviços prestados;**

12.23.3. **Certidão Negativa de Débitos Federais.**

12.23.4. **Certificado de Regularidade do FGTS - CRF.**

12.24. A ausência da documentação supracitada poderá resultar em atrasos no pagamento. Questionamentos poderão ser efetuados no próprio protocolo eletrônico.

12.25. O Protocolo Eletrônico é a forma oficial de pré-agendamento de entrega de produtos, entrega de Notas Fiscais e documentos correlatos junto à EMASA.

12.26. Para tanto, além de anexar eletronicamente tais documentos, o fornecedor deverá fazer uma breve descrição do que será entregue, indicando, entre outros dados, o processo licitatório ou compra direta que gerou a contratação, conforme modelo inicial apresentado no campo "Descrição".

12.27. A EMASA poderá, a qualquer momento, dentro deste mesmo sistema eletrônico de protocolo de notas fiscais, vir a solicitar outros documentos, para que seja possível a liquidação da despesa e o seu consequente pagamento.

12.28. É de responsabilidade exclusiva do fornecedor, o acompanhamento on-line dos trâmites provenientes de seus processos eletrônicos.

12.29. O CARREGAMENTO E/OU DESCARGA DE MATERIAIS, PRODUTOS, OU EQUIPAMENTOS, É DE TOTAL RESPONSABILIDADE DO FORNECEDOR.

12.30. Dúvidas quanto aos procedimentos do protocolo eletrônico, podem ser sanadas através do telefone (47) 3261 0050.

12.31. Todas as alterações que se fizerem necessárias serão registradas por intermédio de lavratura de termo aditivo à presente Ata de Registro de Preços.

13. CLÁUSULA TREZE – DO FORO

13.21. As partes elegem de comum acordo o Foro da cidade de Balneário Camboriú/SC, para dirimir dúvidas ou controvérsias relacionadas com o presente instrumento.

E assim, por estarem de acordo, após terem lido e aceitado todos os termos e condições aqui previstos, assinam o presente contrato em 03 (três) vias de igual teor, para que surta efeito jurídico.

Balneário Camboriú, xxx de xxxx de 2022.

DOUGLAS COSTA BEBER ROCHA	**NOME**
DIRETOR GERAL	**RAZÃO SOCIAL**
EMASA	**FORNECEDOR**

ANEXO A – CADASTRO DE RESERVA

Registro dos licitantes que aceitaram cotar os bens ou serviços com preços iguais aos do licitante vencedor na sequência da classificação do certame, excluído o percentual referente à margem de preferência, conforme decreto municipal nº 8288/16 e art. 64, § 2º da lei nº 8.666/93.

1 - _____

2 - _____

3 - _____

ANEXO III

MODELO

CREDENCIAMENTO

PREGÃO PRESENCIAL Nº 63/2022 – SRP

REGISTRO DE PREÇOS Nº 14/2022

Por este instrumento solicitamos o credenciamento da empresa _____ para participar da licitação acima referenciada, neste evento, representada por (nome/identidade/CPF) _____ ou procuração anexa, na qualidade de REPRESENTANTE LEGAL, outorgando-lhe poderes para pronunciar-se em nome da outorgante, visando formular propostas e lances verbais, negociar preços, declarar a intenção de interposição de recurso, renunciar ao direito de interpor recursos e praticar todos os demais atos inerentes ao certame.

Local e Data

Nome e assinatura do responsável (representante legal)
Cargo
CPF
RG
Carimbo da empresa

OBS.: Documentos a serem apresentados:

(1) em caso de firma individual, o registro comercial;

(2) nos demais casos, o ato constitutivo (estatuto ou contrato social em vigor);

(3) em se tratando de pessoa física, a apresentação da cédula de identidade;

(4) A SER APRESENTADO FORA DOS ENVELOPES DE PROPOSTA E HABILITAÇÃO

ANEXO IV

MODELO

CARTA DE PROPOSTA DE PREÇOS

PREGÃO PRESENCIAL Nº 63/2022 – SRP

REGISTRO DE PREÇOS Nº 14/2022

NOME DA EMPRESA:

ENDEREÇO:

CIDADE: UF: CNPJ Nº :

TELEFONE DA EMPRESA:

CELULAR DO REPRESENTANTE:

BANCO: AGÊNCIA: CONTA CORRENTE:

EMAIL:

OBJETO: REGISTRO DE PREÇOS PARA EVENTUAL CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO PARA PROTEÇÃO INTELIGENTE DE DADOS EM REPOUSO, ESTRUTURADOS E NÃO ESTRUTURADOS, CONTROLE DE ACESSO, VISIBILIDADE E RASTREABILIDADE DE UTILIZAÇÃO DE DADOS EM SERVIDORES DE ARQUIVSOS, BANCO DE DADOS LOCAIS E NUVEM, CUSTÓDIA DE CHAVES CRIPTOGRÁFICAS PARA AMBIENTES EM NUVEM (PÚBLICA, HÍBRIDA OU PRIVADA) COMPOSTA POR SOFTWARES E SERVIÇOS DE GARANTIA E SUPORTE TÉCNICO, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, SERVIÇOS DE TREINAMENTO, SERVIÇOS PARA INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS E SERVIÇOS ESPECIALIZADOS PARA ATENDER ÀS DEMANDAS DA EMASA, CONFORME ESPECIFICAÇÕES TÉCNICAS E DEMAIS CONDIÇÕES CONSTANTES NESTE EDITAL.

PRAZO DE VALIDADE DA PROPOSTA: 60 (sessenta) dias.

FORMA DE PAGAMENTO: Até 30 (trinta) dias após a entrega dos softwares/licenças, mediante apresentação de nota fiscal com toda documentação completa exigida e aprovação da Comissão de Recebimento de Bens, Materiais e Serviços da EMASA.

PRAZO DE ENTREGA: 30 (trinta) dias após o recebimento da Nota de Empenho.

LOCAL DE ENTREGA: A CONTRATADA deverá entregar os itens contratados na sede da EMASA, localizada na Quarta Avenida, n° 250 – Centro – Balneário Camboriú/SC.

VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS: 12 (doze) meses.

“Declaramos expressamente que concordamos com todos os termos e exigências do Edital.”

Lote	ITEM	QTD	Unidade	Descrição da Solução	Métrica	VALOR MÉDIO UNIT - (ANUAL)	VALOR MÉDIO TOTAL (ANUAL)
1	1	4	UN	Fornecimento de agente para proteção de dados para aplicação multiplataforma	Software		
	2	1	UN	Fornecimento de agente para transferência segura de base de dados	Software		
	3	5	UN	Fornecimento de agentes de proteção de dados estruturados multiplataforma	Software		
	4	5	UN	Fornecimento de agentes de proteção de dados não estruturados multiplataforma	Software		
	5	1	UN	Fornecimento de agentes para descoberta e classificação de dados sensíveis - termo de licenciamento por 12 Meses - 15TB	Software		
	6	2	UN	Fornecimento de agentes para gestão de chaves local - 12 meses	Software		
	7	1	UN	Fornecimento de agentes para proteção e custódia de chaves multicloud – termo de licenciamento por 12 meses	Software		
	8	2	UN	Fornecimento de console de gerenciamento de chaves de criptografia em alta disponibilidade	Software		
	9	3	UN	Serviço de Treinamento oficial	Serviço		
	10	12	UN	Serviço de suporte técnico especializado (Helpdesk) – 12 meses	Serviço		
	11	5	UN	Serviço de suporte para agentes de proteção de dados estruturados multiplataforma – 12 meses	Serviço		
	12	5	UN	Serviço de suporte para agentes de proteção de dados não estruturados multiplataforma – 12 meses	Serviço		
	13	4	UN	Serviço de suporte para agentes de proteção de dados para aplicação multiplataforma – 12 meses	Serviço		
	14	2	UN	Serviço de suporte para agentes para gestão de chaves local – 12 meses	Serviço		
	15	2	UN	Serviço de suporte para console de gerenciamento de chaves de criptografia – 12 meses	Serviço		
	16	2	UN	Serviço de Implementação de console de gerenciamento de chaves de criptografia	Serviço		
	17	3000	UST	Serviço sob demanda para Implementação de agentes de criptografia	Serviço		
2	2	12	UN	Serviço de gestão de projetos e documentação - 12 meses	Serviço		
3	3	12	UN	Serviço de análise de risco - 12 meses	Serviço		
4	4	8	UN	Serviço de consultoria para avaliação periódica (HealthCheck)	Serviço		
5	5	12	UN	Serviço de consultoria sob demanda para emissão de relatórios de conformidade com a LGPD - 12 meses	Serviço		
6	6	12	UN	Serviço de diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico	Serviço		
7	7	1	UN	Serviço de suporte de solução para transferência segura de base de dados	Serviço		
					TOTAL		

Nome e assinatura do responsável (representante legal)

Cargo

CPF

RG

Carimbo da empresa

ANEXO V

MODELO

DECLARAÇÃO QUE ATENDE O INCISO V DO ART. 27 DA LEI 8.666/93

PREGÃO PRESENCIAL Nº 63/2022 – SRP

REGISTRO DE PREÇOS Nº 14/2022

_____ (nome da empresa), com sede na _____ (endereço da empresa), CNPJ _____, por seu representante legal infra-assinado, em atenção ao inciso V do art. 27 da Lei 8.666/93, acrescido pela Lei 9.854, de 27 de outubro de 1999, declara, sob as penas da lei, que cumpre integralmente a norma contida no art. 7º, inciso XXXIII, da Constituição da República, ou seja, de que não possui em seu quadro de pessoal, empregado(s) menor(es) de 18 (dezoito) anos, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos.

Local e Data

Nome e assinatura do responsável (representante legal)
Cargo
CPF
RG
Carimbo da empresa

ANEXO VI

MODELO

DECLARAÇÃO DE REGULARIDADE FISCAL

PREGÃO PRESENCIAL Nº 63/2022 – SRP

REGISTRO DE PREÇOS Nº 14/2022

* A SER APRESENTADO FORA DOS DEMAIS ENVELOPES DE PROPOSTA E HABILITAÇÃO

_____(nome da empresa), com sede na _____(endereço da empresa), inscrita no CNPJ sob o nº _____, licitante no certame acima destacado, promovido pela Empresa Municipal de Água e Saneamento de Balneário Camboriú - EMASA, DECLARA, por meio de seu representante legal infra-assinado, R.G. Nº _____, que se encontra em situação regular perante as Fazendas Nacional, Estadual e Municipal, a Seguridade Social (FGTS e INSS), bem como atende às demais exigências de habilitação constantes do edital próprio.

Local de data

Nome e assinatura do responsável (representante legal)
Cargo
CPF
RG
Carimbo da empresa

ANEXO VII

MODELO

INDICAÇÃO DE PREPOSTO

PREGÃO PRESENCIAL Nº 63/2022 – SRP

REGISTRO DE PREÇOS Nº 14/2022

_____ (nome da empresa), com sede na _____ (endereço da empresa), CNPJ _____, participante do Pregão Presencial nº 63/2022, cujo objeto é **REGISTRO DE PREÇOS PARA EVENTUAL CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO PARA PROTEÇÃO INTELIGENTE DE DADOS EM REPOUSO, ESTRUTURADOS E NÃO ESTRUTURADOS, CONTROLE DE ACESSO, VISIBILIDADE E RASTREABILIDADE DE UTILIZAÇÃO DE DADOS EM SERVIDORES DE ARQUIVSOS, BANCO DE DADOS LOCAIS E NUVEM, CUSTÓDIA DE CHAVES CRIPTOGRÁFICAS PARA AMBIENTES EM NUVEM (PÚBLICA, HÍBRIDA OU PRIVADA) COMPOSTA POR SOFTWARES E SERVIÇOS DE GARANTIA E SUPORTE TÉCNICO, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, SERVIÇOS DE TREINAMENTO, SERVIÇOS PARA INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS E SERVIÇOS ESPECIALIZADOS PARA ATENDER ÀS DEMANDAS DA EMASA, CONFORME ESPECIFICAÇÕES TÉCNICAS E DEMAIS CONDIÇÕES CONSTANTES NESTE EDITAL, informa** por meio deste que é a pessoa designada pela empresa para que a represente na relação contratual a ser estabelecida com a EMASA, caso seja vencedora deste certame, conforme o que segue abaixo:

PREPOSTO

Nome: _____

Endereço: _____

CPF:_____ RG: _____

Celular: _____

Email: _____

Nome e assinatura do responsável (representante legal)

Cargo

CPF

RG

Carimbo da empresa

ANEXO VIII

MODELO

DECLARAÇÃO DE ENQUADRAMENTO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

PREGÃO PRESENCIAL Nº 63/2022 – SRP

REGISTRO DE PREÇOS Nº 14/2022

* A SER APRESENTADO FORA DOS DEMAIS ENVELOPES DE PROPOSTA E HABILITAÇÃO

_____, inscrita no CNPJ sob o nº __ _____, por intermédio de seu representante legal, o(a) Sr.(a.) _____, portador(a) da Carteira de Identidade nº _____, do CPF nº _____, DECLARA, para fins do disposto no subitem 4.11 do Edital de Pregão Presencial nº ___/2022, sob as sanções administrativas cabíveis e sob as penas da lei, que esta empresa, na presente data, é considerada:

( ) MICROEMPRESA, conforme inciso I do art. 3º da Lei Complementar nº 123 de 14/12/2006 e que não ultrapassou limite do faturamento.

( ) EMPRESA DE PEQUENO PORTE, conforme inciso II do art. 3º da Lei Complementar nº 123 de 14/12/2006 e que não ultrapassou limite do faturamento.

Declara ainda que a empresa está excluída das vedações constantes do § 4º do art. 3º da Lei Complementar nº 123 de 14 de dezembro de 2006.

_____, ____ de _____ de 2022.

Nome e assinatura do responsável (representante legal)
Cargo
CPF
RG
Carimbo da empresa

OBSERVAÇÃO:
Assinalar com um “X” a condição da empresa.

ANEXO IX

MODELO

DECLARAÇÃO DE AUSÊNCIA DE PARENTESCO

PREGÃO PRESENCIAL Nº 63/2022 – SRP

REGISTRO DE PREÇOS Nº 14/2022

_____, inscrita no CNPJ sob o nº __ _____, por intermédio de seu representante legal, o(a) Sr.(a.) _____, portador(a) da Carteira de Identidade nº _____, do CPF nº _____, DECLARA:

1) Não possuir proprietário, sócios ou funcionários que sejam servidores ou agentes políticos da EMPRESA MUNICIPAL DE ÁGUA E SANEAMENTO DE BALNEÁRIO CAMBORIÚ;

2) Não possuir proprietário ou sócio que seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, e por afinidade, até o segundo grau, de agente político da EMPRESA MUNICIPAL DE ÁGUA E SANEAMENTO DE BALNEÁRIO CAMBORIÚ – EMASA.

_____, ____ de _____ de 2022.

Nome e assinatura do responsável (representante legal)
Cargo
CPF
RG
Carimbo da empresa
OBSERVAÇÃO:

OBS: Para fins de conhecimento, entenda-se por "**AGENTE POLÍTICO**" os cargos que foram nomeados pelo Prefeito Municipal de Balneário Camboriú/SC para atuar na EMASA (diretores, gerentes, coordenadores, etc.).

AVISO DE LICITAÇÃO
PREGÃO PRESENCIAL Nº 63.2022

OBJETO: REGISTRO DE PREÇOS PARA EVENTUAL CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO PARA PROTEÇÃO INTELIGENTE DE DADOS EM REPOUSO, ESTRUTURADOS E NÃO ESTRUTURADOS, CONTROLE DE ACESSO, VISIBILIDADE E RASTREABILIDADE DE UTILIZAÇÃO DE DADOS EM SERVIDORES DE ARQUIVSOS, BANCO DE DADOS LOCAIS E NUVEM, CUSTÓDIA DE CHAVES CRIPTOGRÁFICAS PARA AMBIENTES EM NUVEM (PÚBLICA, HÍBRIDA OU PRIVADA) COMPOSTA POR SOFTWARES E SERVIÇOS DE GARANTIA E SUPORTE TÉCNICO, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, SERVIÇOS DE TREINAMENTO, SERVIÇOS PARA INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS E SERVIÇOS ESPECIALIZADOS PARA ATENDER ÀS DEMANDAS DA EMASA, CONFORME ESPECIFICAÇÕES TÉCNICAS E DEMAIS CONDIÇÕES CONSTANTES NESTE EDITAL**.**
Tipo de licitação: Menor Preço por Lote.
Entrega dos envelopes: até às 10:30 horas (Horário de Brasília) do dia 07 de dezembro de 2022.
Data e horário de abertura: às 10:40 horas (Horário de Brasília) do dia 07 de dezembro de 2022.
Local: Sede administrativa da EMASA – 4ª Avenida, 250, Centro, Balneário Camboriú/SC.
RETIRADA DO EDITAL: http://emasa.com.br/emasa/licitacoes/licitacoes

Balneário Camboriú, 23 de novembro de 2022.

Douglas Costa Beber Rocha
Diretor Geral

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 1144-2DE7-5DB8-0E4F

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

DOUGLAS COSTA BEBER ROCHA (CPF 985.XXX.XXX-34) em 23/11/2022 13:48:51 (GMT-03:00)
Papel: Parte
Emitido por: Autoridade Certificadora SERPRORFBv5 << AC Secretaria da Receita Federal do Brasil v4 << Autoridade Certificadora Raiz Brasileira v5 (Assinatura ICP-Brasil)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://emasa.1doc.com.br/verificacao/1144-2DE7-5DB8-0E4F