ESTADO DE ALAGOAS

INSTITUTO DE TECNOLOGIA EM INFORMATICA E INFORMAÇÃO

Gerência de Operações
Rua Cincinato Pinto, 503, - Bairro Centro, Maceió/AL, CEP 57017-160
Telefone: (82) 3315-1533 - www.itec.al.gov.br

TERMO DE REFERÊNCIA – BENS

TERMO DE REFERÊNCIA – BENS

PREGÃO ELETRÔNICO Nº (...)/(20...)

Processo Administrativo n° (41506.00000000507/2021)

1. DA APRESENTAÇÃO

1.1. À Agência de Modernização da Gestão de Processos – AMGESP, nos termos da Lei Estadual nº 6.582, de 2005, compete as atividades de execução, acompanhamento e controle referentes a compras de materiais e contratação de serviços da Administração Pública Estadual direta e indireta, inclusive por meio do Sistema de Registro de Preços, regulamentado pelo Decreto nº 68.120, de 2019.

1.2. A Agência de Modernização da Gestão de Processos – AMGESP desempenhará as funções do Órgão Gerenciador, responsável pela condução do conjunto de procedimentos para registro de preços e gerenciamento da ata de registro de preços dele decorrente.

1.3. Art. 3º O SRP poderá ser adotado nas seguintes hipóteses:

1.3.1. Quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;

1.3.2. Quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;

1.3.3. Quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de 1 (um) órgão ou entidade, ou a programas de governo; ou

1.3.4. Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela administração.

1.4. A Ata de Registro de Preços, decorrente do registro de preços, é documento vinculativo, obrigacional, com característica de compromisso para futura

contratação, em que se registram os preços, fornecedores, órgãos participantes e condições a serem praticadas, conforme as disposições contidas no instrumento convocatório e propostas apresentadas.

1.5. A existência de preços registrados não obriga a Administração a contratar, facultando-se a realização de licitação específica para a contratação pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

2. DO OBJETO

2.1. A presente solicitação tem por objetivo a criação de ata de registro de preços (SRP), para aquisição de SOLUÇÃO DE SEGURANÇA DE E-MAIL COM ANTISPAM E ANTIVÍRUS E ROTEADOR DE BORDA, incluindo licenciamento e garantia da solução, que permitirá compor um conjunto fluído de recursos físicos e virtuais de computação, exclusivo para este ITEC, conforme condições, quantidades e exigências a seguir estabelecidas:

Lote	Catmat/ catser	Descrição	Unidade de Medida	Quantidade
Lote único (segurança e conectividade)	104620	Roteador de borda internet, incluindo licenciamento e garantia da solução, conforme descrito no item 17 deste termo de referência	UND	04
	27464	Firewall Antispam, e antivírus, incluindo licenciamento e garantia da solução, conforme descrito no item 17 deste termo de referência	UND	04

2.2. A presente contratação terá vigência de 12(doze) meses, contado da data de publicação do extrato contratual no Diário Oficial do Estado, a partir de quando as obrigações assumidas pelas partes serão exigíveis, sendo prorrogável na forma do art. 57, §1º, da Lei nº 8.666, de 1993.

2.3. Todos os equipamentos no que diz respeito a hardware, devem possuir garantia técnica, suporte técnico e atualização de software dos respectivos fabricantes, por no mínimo de 36 (trinta e seis) meses, conforme Lei 8.666/96, contra defeito de fabricação dos equipamentos, os quais não caracteriza serviço continuado, e assim ocorra a correta implantação e manutenção das plataformas do Datacenter do ITEC. Também devem ser fornecidos serviços de instalação, serviços customizados de integração e migração, e transferência de conhecimento técnico.

2.3.1. Todos os equipamentos no que diz respeito a licenças de uso de software de forma perpetua, devem ter garantia de 60 (sessenta) meses do desenvolvedor do software, conforme Lei 8.666/96, para a correta implantação e manutenção das plataformas do Datacenter do ITEC. Também devem ser fornecidos serviços de instalação, serviços customizados de integração e migração, suporte técnico, atualização de software e transferência de conhecimento técnico para os softwares fornecidos.

2.3.2. Para assegurar a eficiência da SOLUÇÃO que será adquirida, a integração dos componentes (hardwares e softwares) precisa ser garantida pelo próprio fabricante dos equipamentos e softwares. Contudo, para aumentar a competitividade do

certame, serão admitidas ofertas de soluções de mais de um fabricante, desde que o fornecedor comprove sua competência técnica como provedor de soluções dos fabricantes que fazem parte da solução ofertada por ela, bem como garantir a interoperabilidade entre os componentes (hardwares e softwares).

2.3.3. A contratação será pontual, sob demanda e é parte inerente da solução que será ofertada por cada empresa proponente.

2.4. O prazo de garantia do equipamento a ser adquirido terá início quando da data de entrega definitiva do mesmo. No caso de haver defeitos nas peças, e se, consequentemente, houver substituição, a garantia de tais peças será a mesma do equipamento onde tiver sido instalada.

3. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. O ITEC é a autarquia responsável pela proposição e execução da Política Estadual de Informática e Informação; pela execução dos serviços corporativos do Estado e gestão da rede de comunicação de dados, voz e imagem da Administração Pública, promovendo o assessoramento na informatização dos órgãos governamentais na elaboração e execução de seus programas e projetos de modernização institucional e na utilização da tecnologia da informática e informação; pelo planejamento, desenvolvimento, implantação, manutenção e orientação nas demandas de produtos e serviços relativos ao uso da tecnologia da informática e informação, prestando consultoria relativa ao planejamento das atividades dos órgãos setoriais e vinculados.

3.2. Com a evolução e o desenvolvimento de novas aplicações e serviços informatizados na rede corporativa do ITEC/AL, novos serviços e sistemas, disponibilizados aos inúmeros usuários, internos e externos à organização, e as mais diversas secretarias, vêm-se registrando o esgotamento dos recursos da infraestrutura de armazenamento computacional e banco de dados que suportam esses serviços.

3.3. O constante crescimento da demanda por tecnologia da informação, serviços e infraestrutura para novos ou já existentes sistemas, exige hoje do ITEC, muita flexibilidade e maturidade tecnológica para poder atendê-las de forma rápida, segura e racional.

3.4. Diante, do avanço das ameaças cibernéticas, cada vez mais atuante no meio governamental, as ferramentas de segurança da informação também precisam se tornar cada vez mais diversas e sofisticadas no combate do avanço das invasões da rede. Com a solução pretendida, o firewall protegerá a rede em conjunto ao AntiSpam e antivírus que focarão em bloquear as ameaças que chegam via e-mail e inspecionará os arquivos que estão instalados ou prestes a ser instalado no computador, verificando a existência de arquivos maliciosos ou corrompidos.

3.5. Atualmente no Data Center do ITEC, vem ocorrendo uma significativa necessidade de ampliação do sistema de segurança, em sua infraestrutura de rede e de processamento. Dessa forma, a alta manutenção do nível, deste serviço, se tornou igualmente crítica, fazendo com que a disponibilidade da infraestrutura computacional seja altamente relevante, para mantermos a máquina pública segura de ataques maliciosos.

3.6. Insto salientar, dá importância da solução pretendida, que nos possibilitará uma segurança mais ampla para a rede principal, sendo como um ponto de acesso aos demais dados (conectividade), no ajudando no controlo do fluxo de informações dentro e fora da rede, diminuindo as falhas do sistema e melhorando a velocidade e encaminhando os dados de uma rede a outra (interna a externa).

3.7. Em reforço ao item 2.1 (tabela do objeto) os itens constantes, atendendo ao Marco Civil, nos habilitará a implementar controles para atendimento à LGPD (Lei Geral de Proteção aos Dados), os quais responsabilizam aos gestores por vazamentos de dados, falhas de segurança entre outras pragas virtuais.

3.8. Tendo em vista as novas leis promulgadas pelo governo federal LEI 13.790/2018 que trata da LGPD e Lei 19.965/2014 do Marco Civil, as empresas proponentes deverão discriminar como a solução ofertada habilitará o ITEC a cumprir ambas as Leis.

3.9. A presente aquisição é imprescindível para garantir alto desempenho dos sistemas e serviços do GOVERNO DO ESTADO DE ALAGOAS, mais precisamente citamos como exemplo: **SEI, FOLHA DE PAGAMENTO, ALMOXARIFADO, SISTEMAS HOSPITALARES, SITES GOVERNAMENTAIS, SISTEMA DE ARRECADAÇÃO, Sistemas do DETRAN, SERVIÇOS DE SEGURANÇA PÚBLICA, Sistemas do BOMBEIRO, SISTEMAS DE INTELIGÊNCIA, IDENTIFICAÇÃO CIVIL E CRIMINAL, TELE TRABALHO, SITES INSTITUCIONAIS, DENTRE OUTROS INUMEROS SERVIÇOS**, que possam estar em produção a contento, processando com bom desempenho as demandas diárias, bem como para efetuar as tarefas rotineiras que são necessárias para realização dos trabalhos prestados pelo ITEC.

3.10. Ademais, após a uma análise técnica minuciosa do atual Datacenter do Estado, este ITEC, chegou à conclusão irrefutável da necessidade de modernizá-lo com as mais atuais tecnologias dispostas no mercado, no que cerne em segurança de rede. Pois com a ocorrência de tantos ataques cibernéticos aos órgãos governamentais, é imprescindível a aquisição de uma solução de segurança, que garantam, que os serviços e sistemas possam operarem em alta disponibilidade de forma segura a todos que utilizam o Datacenter do Governo do Estado de Alagoas.

3.11. Buscando atender o compromisso do Governo do Estado do Estado, em garantir eficiência da gestão pública, é essencial a aquisição de um novo dispositivo de Data Center em conjunto ao grupo de geradores. Visando obter um ambiente computacional renovado e confiável, atendendo desta forma, as normas internacionais de segurança e com garantias nos serviços desenvolvidos e disponibilizados por este instituto.

3.12. O ITEC precisa estar fortalecido em TIC para oferecer suporte tecnológico às entidades que têm a missão de atender aos anseios e expectativas da População (Serviços Públicos), do Governo (Governo Digital) e dos seus Servidores (Técnicos e Usuários), estando o Estado preparado para o futuro e para as futuras gerações.

3.13. Ao que se refere, na questão de licença de uso de software, este não pode ser considerado como serviço e sim como bem imaterial, uma vez que, no momento da sua aquisição se obtém de forma perpetua e definitiva ao hardware a ser adquirido, ou seja, indo de encontro ao que se refere a contratação de serviço, que se tem tempo pré-definido de acordo com a Lei 8.666/94.

3.14. Onde após análise técnica, pudemos averiguar que parte do parque computacional, está defasado tecnologicamente e com uma demanda reprimida. A consequência desta evolução, se reflete diretamente no bom funcionamento de sistemas críticos e essenciais a todos, além de poder ocasionar em inúmeras falhas nos serviços. E com uma infraestrutura de rede confiável e com capacidade necessária para as aplicações mais críticas, podemos atender com segurança e desempenho as demandas atuais do Estado.

3.15. Tornando-se cada vez mais indispensável ao ITEC, garantir a proteção de todos os dados governamentais e assim evitando que as ameaças atinjam a rede corporativa, que causariam prejuízos inestimáveis a máquina pública do Estado. Com

isso, promoveremos a eficiência e a consolidação dos investimentos em uma plataforma centralizada, segura, padronizada e com um alto desempenho projetado para o Data Center atual e um novo dispositivo a ser adquirido por este Instituto.

3.16. Pretende-se adquirir o presente objeto por meio do Sistema de Registro de Preço, em razão da necessidade de atender as demandas, deste ITEC, bem como as demandas dos órgãos e entidades da Administração Pública de Alagoas, em cumprimento ao Decreto nº. 35.143/2014. De modo que, a implantação da infraestrutura do dispositivo datacenter/grupo de geradores para melhor performance contínua e capacidade técnica e atual para atendimento ao Estado. Onde será em acordo com a disponibilidade financeira do Estado para investimentos e as demandas pelo ITEC, além dos cronogramas de migração que serão elaborados. Portanto, como há necessidade de contratações frequentes com entregas parceladas, incluindo a remuneração por disposto adquirido, adotamos o SRP (Sistema de Registro de Preços), de forma assegurar a compatibilidade entre os componentes ofertados para a infraestrutura descritas neste termo de referência.

4. CLASSIFICAÇÃO DOS BENS COMUNS

4.1. A natureza do objeto a ser contratado é comum, nos termos do parágrafo único do art. 1° da Lei 10.520, de 2002.

5. DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Dentre outros, são documentos de habilitação compatíveis com as peculiaridades do objeto da licitação:

5.1.1. As empresas proponentes deverão comprovar capacidade técnica e operacional de assistência técnica, com atendimento “On site”, relativa ao objeto ofertado. Devendo ser identificado e comprovado que a empresa é autorizada pelo fabricante a prestar a assistência técnica do bem, e apresentar a aptidão para o fornecimento dos bens em características, quantidades e prazos compatíveis com o objeto da licitação, digam respeito a contratos executados com os mesmos aspectos: e que possam comprovar através de contratos, atestados e declarações fornecidas por entidades públicas ou privadas reconhecidas.

5.1.2. Para a futura e eventual aquisição, não haverá necessidade da exigência de patrimônio líquido mínimo para habilitação, de acordo com os dados obtidos no mercado sobre a área do objeto da contratação e o porte das empresas que nela atuam, e considerando a ausência de maior risco para a Administração.

5.1.2.1. Ademais a empresa vencedora só receberá o pagamento, após a entrega do objeto pretendido deste termo de referência. Visto que, o certame será promovido através de SRP (sistema de registo de preço), onde só será adquirido pelo órgão, de acordo com a disponibilidade financeira do Estado para investimentos e as demandas pelo ITEC, devido a isso e afim de aumentar a competividade do certame, não será exigido a comprovação de patrimônio líquido.

5.1.3. Atestados fornecidos por pessoas jurídicas de direito público ou privado que, comprovando aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto da licitação, digam respeito a contratos executados com os seguintes aspectos:

5.1.3.1. Atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando a instalação, configuração e manutenção de roteador de borda de internet e firewall de antispam/antivírus, ambos em alta disponibilidade, em um datacenter de abrangência estadual, ou equivalente para entrega dos serviços técnicos especializados.

5.1.3.2. Características: fornecimento de todos os componentes do Roteador de

borda internet e Firewall Antispam, e antivírus , incluindo garantia e licenciamento da solução. Todos os equipamentos deverão ser novos, encontrados em linha de produção do fabricante (não descontinuados) na data de entrega dos equipamentos e homologados pela Anatel (se assim os tiver), e que todas as licenças de software ofertadas deverão ser perpétuas, permitindo a continuidade do funcionamento do sistema, ainda que não cobertas por contrato de atualização, suporte e subscrição de base de dados de segurança. Devendo conter Lista de Itens Ofertados com *PartNumbers* (código do produto do fabricante) / Quantidade / Fabricante / Descrição, inclusive dos serviços de garantia, software e suporte técnico do fabricante.

5.1.3.3. Referindo-se a execução dos serviços técnicos, estes deverão ser realizados por prestador de serviços com vínculo contratual (sem vínculo trabalhista e regido pela legislação civil (Acórdão TCU 2652/2019-Plenário)/ ou por profissional, já existente no quadro de funcionários ou por sócio da empresa vencedora, onde em ambos os casos, os técnicos devem ser habilitados e certificados pelo fabricante, que comprovem estarem aptos a desenvolverem os serviços técnicos em gerência de projetos PMP (Project Manager Professional) emitida pelo PMI (Project Management Institute); PMBOK (Project Management Body of Knowledge), Certificação em ITIL Fundantion; Certificação CBPP (Certified Business Process Professional) emitida pela ABPMP (Associação dos Profissionais de Gerenciamento de Processos); Certificação do fabricante para os produtos ofertados, ou equivalente para entrega dos serviços técnicos, devido à especificidade dos sistemas e softwares integrados ao hardware, para garantir a interoperatividade da solução adquirida.

5.1.3.4. Quantidades: no mínimo de 50% (cinquenta por cento) da quantidade do objeto licitado.

5.1.3.5. Prazos: no máximo, 50% (cinquenta por cento) superior ao prazo de entrega do objeto licitado.

5.1.4. As empresas proponentes deverão comprovar atendimento a todas as exigências técnicas do Termo de Referência através de documentação pública, datasheets, folders, manuais, ou declarações especificas do fabricante dos equipamentos e/ou desenvolvedores dos softwares, inclusive das exigências de Service Level Agreement (SLA), da garantia que deve ser do próprio fabricante.

5.1.5. As empresas proponentes deverão apresentar comprovação de que o fabricante dos equipamentos prestará a assistência/suporte técnico para os produtos ofertados, inclusive com os Service Level Agreements (SLAs) exigidos, ainda que, os atendimentos locais sejam através de rede autorizada (indicar a autorizada local - constando nome e telefone de contato dos responsáveis). Não serão aceitas declarações genéricas.

5.1.6. Os atestados de capacidade técnica estarão sujeitos à diligência por parte da comissão de licitação, que poderá averiguar através de visita técnica, a autenticidade das informações. Se durante este processo, for constatada fraude em qualquer um dos documentos, a licitante envolvida estará automaticamente desclassificada do processo licitatório em questão, além de estar sujeita às penalidades da lei.

5.1.7. Os atestados referir-se-ão a contratos já concluídos ou já decorridos no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior.

5.1.8. A seu critério, o ITEC poderá realizar diligências para validar comprovações apresentadas. Independentemente das comprovações que servirão para aceitação ou não das propostas, todas exigências serão revalidadas quando do recebimento dos produtos e certificados.

6. DA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

6.1. O prazo de entrega dos bens é de 30 (trinta) dias, contados do efetivo recebimento da Ordem de Fornecimento, em remessa única ou parcelada, de acordo com a necessidade do órgão participante, obedecendo, se for o caso, ao cronograma físico-financeiro das entregas parceladas por ele estabelecido, na Rua Cincinato Pinto, 503 – Centro – Maceió/AL na sede do ITEC de segunda a sexta-feira, das 08:00 às 16:00 horas.

6.1.1. Caso o prazo de entrega venha a ultrapassar os 30(trinta) dias, este pode ser prorrogado em igual ou menor prazo acima mencionados, nas condições do § 1º, do art. 57 da Lei nº 8.666/93, desde que justificado por escrito e previamente autorizado pelo Presidente do ITEC.

6.2. No caso de produtos perecíveis, o prazo de validade na data da entrega não poderá ser inferior a 75% (setenta e cinco por cento) do prazo total recomendado pelo fabricante.

6.3. Os bens serão recebidos provisoriamente no prazo de 5 (cinco) dias úteis, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

6.4. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da Contratada, às suas custas, sem prejuízo da aplicação das penalidades.

6.5. Os bens serão recebidos definitivamente no prazo de 10 (dez) dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

6.6. Na hipótese de não se proceder à verificação a que se refere o subitem anterior dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

6.7. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

6.8. Ao assinar o contrato, a empresa vencedora assume o compromisso de obedecer ao "termo de ciência das regras de segurança e termo de compromisso, sigilo e confidencialidade", conforme anexo I e II, bem como os normativos dela decorrente, mantendo a mais absoluta confidencialidade sobre materiais, dados e informações disponibilizados ou conhecidos em decorrência do contrato assinado.

7.0. OBRIGAÇÕES DA CONTRATANTE

7.1. São obrigações da contratante:

7.1.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

7.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

7.1.3. Comunicar à contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

7.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da contratada, através de comissão/servidor especialmente designado;

7.1.5. Efetuar o pagamento à contratada no valor correspondente ao fornecimento

do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

7.2. A Administração não responderá por quaisquer compromissos assumidos pela contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos ou subordinados.

8. OBRIGAÇÕES DA CONTRATADA

8.1. A contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

8.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

8.1.1.1. O objeto deve estar acompanhado do manual do usuário, com uma versão em português ou inglês e da relação da rede de assistência técnica autorizada, quando for o caso;

8.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

8.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado no Termo de Referência, o objeto com avarias ou defeitos;

8.1.4. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

8.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

8.1.6. Renovar, durante a vigência do contrato, a cada 6 meses, a Declaração de Cumprimento de Cota de Aprendizagem – DCCA, conforme o art. 429 da Consolidação das Leis do Trabalho – CLT, acompanhada da última informação do Cadastro Geral de Empregados e Desempregados (CAGED), ou do Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas – eSocial, e do número de contratação de jovens aprendizes;

8.1.6.1. Ficam liberadas de renovar DCCA e documentos complementares as microempresas e empresas de pequeno porte;

8.1.7. Indicar preposto para representá-la durante a execução do contrato.

8.1.8. A contratada deve cumprir todos os requisitos técnicos exigidos no item 17 deste termo de referência.

9. SUBCONTRATAÇÃO

9.1. Não será admitida a subcontratação do objeto licitatório.

10.0. ALTERAÇÃO SUBJETIVA

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

11. DO GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS

11.1. A Agência de Modernização da Gestão de Processos – AMGESP desempenhará as funções do Órgão Gerenciador da Ata de Registro de Preços, cabendo-lhe a prática de todos os atos de controle e administração, inclusive:

11.1.1. Providenciar a assinatura da Ata de Registro de Preços.

11.1.2. Conduzir eventuais renegociações dos preços registrados e, em sendo o caso, revogar a Ata de Registro de Preços;

11.1.3. Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na Ata de Registro de Preços;

11.1.4. Anuir à utilização da Ata de Registro de Preços, durante sua vigência, por Órgão Não Participante;

11.1.5. Autorizar, excepcional e justificadamente, a prorrogação do prazo para o Órgão Não Participante efetivar a aquisição ou contratação solicitada, respeitado o prazo de vigência da Ata de Registro de Preços;

11.1.6. Formalizar o cancelamento do registro do fornecedor.

11.2. No gerenciamento da Ata de Registro de Preços, haverá prioridade de aquisição dos produtos das cotas reservadas, ressalvados os casos em que a cota reservada for inadequada para atender às quantidades ou às condições do pedido, justificadamente.

12. DO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

12.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

12.1.1. O recebimento de material de valor superior a R$ 176.000,00 (cento e setenta e seis mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente.

12.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios e, na ocorrência desta, não implica corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

12.2.1. Serão designados para exercerem a função de gestores e fiscais contratuais os servidores José Álvaro de Oliveira - matrícula 53.231-2, Paulo Silva Coutinho - matrícula 052-7 e Raymundo Sampaio Fernandes - matrícula 033-7, denominados Comissão Gestora.

12.2.2. A fiscalização e gestão de todo lote 02, não ficará sob a responsabilidade do servidor José Álvaro de Oliveira - matrícula 53.231-2, cabendo aos demais servidores da comissão gestora, acima já citados e denominados de exercerem a gestão e fiscalização deste lote.

12.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

13. DO PAGAMENTO

13.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, acompanhada da comprovação da regularidade fiscal, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela Contratada.

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

13.2. Considera-se ocorrido o recebimento da Nota Fiscal ou Fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

13.3. Havendo erro na apresentação da Nota Fiscal ou Fatura ou dos documentos pertinentes à contratação ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente 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 a Contratante.

13.4. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

13.5. Antes da emissão de Nota de Empenho e a cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital por ele abrangidas ou, na impossibilidade de acesso ao referido Sistema, consulta aos sítios eletrônicos oficiais ou à documentação mencionada nos arts. 28, 29 e 31 da Lei nº 8.666, de 1993.

13.5.1. Na mesma oportunidade, a Administração realizará consulta ao SICAF, à Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União e ao Cadastro das Empresas Inidôneas, Suspensas e Impedidas do Estado de Alagoas – CEIS para identificar eventual proibição de contratar com o Poder Público.

13.6. A renovação, durante a vigência do contrato, a cada 6 meses, da Declaração de Cumprimento de Cota de Aprendizagem – DCCA, conforme o art. 429 da Consolidação das Leis do Trabalho – CLT, acompanhada da última informação do Cadastro Geral de Empregados e Desempregados (CAGED), ou do Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas – eSocial, e do número de contratação de jovens aprendizes, é condição do pagamento.

13.6.1. Ficam liberadas de renovar DCCA e documentos complementares as microempresas e empresas de pequeno porte.

13.7. Constatando-se a situação de irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 10 (dez) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa.

13.8. Não havendo regularização ou sendo a defesa considerada improcedente, a Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da Contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

13.9. Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

13.9.1. Será rescindido o contrato em execução com a Contratada inadimplente,

salvo por motivo de economicidade, segurança nacional ou interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da Contratante.

13.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a Contratada não regularize sua situação.

13.11. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

13.11.1. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

14. DO REAJUSTE

14.1. Os preços são fixos e irreajustáveis.

14.2. Na hipótese de prorrogação extraordinária, na forma do art. 57, §1º, da Lei nº 8.666, de 1993, fica assegurada a manutenção de seu equilíbrio econômico-financeiro, aplicando-se o índice INPC (Índice Oficial para Correção Monetária), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, contada da data limite para a apresentação das propostas.

15. DA GARANTIA DE EXECUÇÃO

15.1. Não haverá exigência de garantia de execução para a contratação.

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. Pratica ato ilícito, nos termos da Lei nº 10.520, de 2002, o licitante ou a Contratada que:

16.1.1. Não assinar o contrato ou a ata de registro de preço;

16.1.2. Não entregar a documentação exigida no edital;

16.1.3. Apresentar documentação falsa;

16.1.4. Causar o atraso na execução do objeto;

16.1.5. Não mantiver a proposta;

16.1.6. Falhar na execução do contrato;

16.1.7. Fraudar a execução do contrato;

16.1.8. Comportar-se de modo inidôneo;

16.1.9. Declarar informações falsas; e

16.1.10. Cometer fraude fiscal.

16.2. As sanções do subitem 16.1. também se aplicam aos integrantes do cadastro de reserva em Pregão para Registro de Preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.

16.3. A prática de ato ilícito sujeita o infrator à aplicação das seguintes sanções administrativas, sem prejuízo da possibilidade de rescisão contratual, nos termos da Lei nº 10.520, de 2002, e do Decreto nº 68.119, de 2019:

16.3.1. Impedimento de licitar e contratar com o Estado de Alagoas e

descredenciamento nos seus sistemas cadastrais de fornecedores, por prazo não superior a 5 (cinco) anos; e

16.3.2. Multa.

16.4. A multa pode ser aplicada isolada ou cumulativamente com as sanções de impedimento de licitar e contratar com o Estado de Alagoas e descredenciamento nos seus sistemas cadastrais de fornecedores, sem prejuízo de perdas e danos cabíveis.

16.5. Se, durante o processo de aplicação de sanção, houver indícios de prática de ato ilícito tipificado pela Lei nº 12.846, de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

16.5.1. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Estadual resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

16.6. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do infrator, o Estado de Alagoas ou a Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

16.7. A aplicação de qualquer das sanções previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante ou à Contratada, observando-se o procedimento previsto no Decreto nº 68.119, de 2019, e subsidiariamente na Lei nº 6.161, de 2000.

16.8. A autoridade competente, na aplicação das sanções, levará em consideração a natureza e a gravidade do ato ilícito cometido, os danos que o cometimento do ato ilícito ocasionar aos serviços e aos usuários, a vantagem auferida em virtude do ato ilícito, as circunstâncias gerais agravantes e atenuantes e os antecedentes do infrator, observado o princípio da proporcionalidade.

16.9. As sanções serão obrigatoriamente registradas no Cadastro das Empresas Inidôneas, Suspensas e Impedidas do Estado de Alagoas – CEIS.

17. DAS ESPECIFICAÇÕES TÉCNICAS E FUNCIONALIDADES PARA A SOLUÇÃO DE SEGURANÇA DE E-MAIL COM ANTISPAM E ANTIVÍRUS E ROTEADOR DE BORDA, LOTE ÚNICO.

17.1. A descrição da solução como um todo abrange: (Todas as informações técnicas compartilhadas refletem produtos/serviços, com configurações/ características e qualidades mínimas aceitáveis para este ITEC, as soluções fornecidas podem ser iguais ou superiores as mensuradas neste termo de referência, visando obter um ambiente computacional adequado, atendendo as normas internacionais de segurança e garantir os serviços desenvolvidos e disponibilizados por este instituto, de forma eficiente e eficaz para todo o Estado. Em que, atualmente existe no mercado diversas marcas que é disponibilizada de forma similar por vários fabricantes, ao qual podem serem aceitadas ou não, a depender se tais soluções correspondem as especificidades mínimas abaixo, demonstrando que não existe forma restritiva a competividade ao certame).

17.1.1. LOTE ÚNICO – DAS CONFIGURAÇÕES TÉCNICAS COMUNS MÍNIMAS DO ROTEADOR DE BORDA INTERNET, COMO;

17.1.2. Deve ser instalável em rack padrão 19” e possuir no máximo 2RU de altura.

17. Deve possuir, no mínimo, 8 (oito) interfaces 10 Gbps SFP+;

17. Deve possuir, no mínimo, 8 (oito) interfaces 1 Gbps SFP;

17. Deve possuir 1 (um) slot disponível para expansão de portas;

17.31.5. Deverão ser fornecidos todos licenciamentos e transceivers SFP+ necessários para ativar 8 portas 10 Gbps Short Range;

17.31.6. Deverão ser fornecidos todos licenciamentos e transceivers SFP necessários para ativar 8 portas 1 Gbps Short Range;

17.31.7. Deve possuir, no mínimo, 2 (duas) fontes internas redundantes com 700W AC;

17.31.8. Deve suportar módulo de criptografia com capacidade para até 20 Gbps de throughtput criptografado;

17.31.9. Deve possuir arquitetura de encaminhamento centralizada e arquitetura de controle distribuído.

17.31.10. Deve suportar roteamento de sistemas autônomos com duas operadoras distintas utilizando protocolo BGP versão 4 full-routing (tabela de roteamento completa).

17.31.11. Deve aceitar designações de números AS de 4 bytes e 2 bytes nativamente.

17.31.12. Deve possuir suporte a Inserção e Remoção Online (OIR) de módulos, ou tecnologia equivalente.

17.31.13. Deve possuir suporte a Nonstop Forwarding (NSF) e Stateful Switchover (SSO), ou tecnologias equivalentes.

17.31.14. Deve implementar VLANs por porta compatível com o padrão IEEE 802.1q;

17.31.15. Deve implementar roteamento: estático, OSPF, BGP e PBR (Policy Base Routing);

17.31.16. Deve implementar protocolo de tunelamento GRE;

17.31.17. Deve implementar listas de controle de acesso (ACLs), baseados em endereço IP de origem e destino, portas TCP e/ou UDP de origem e destino, ou mecanismo de controle de acesso baseados em parâmetros de sockets de rede (IP, Porta de Serviço);

17.31.18. Implementar o protocolo NTPv4 (Network Time Protocol, versão 4).

17.31.19. Deve possuir capacidade de encaminhamento de no mínimo 80 Gbps.

17.31.20. Deve suportar, no mínimo, 5.800 (cinco mil e oitocentos) túneis Ipsec;

17.31.21. Deve suportar, no mínimo, 5.800 (cinco mil e oitocentos) túneis GRE;

17.31.22. Deve suportar, no mínimo, 250 (duzentas e cinquenta) VRFs;

17.31.23. Deve possuir escalabilidade para até 3.500.000 (três milhões e quinhentas mil) de rotas IPv4 ou 3.000.000 (três milhões) de rotas IPv6.

17.31.24. Deve possuir escalabilidade para 250.000 (duzentas e cinquenta mil) entradas na tabela ARP;

17.31.25. Deve suportar, no mínimo, 2.000 ACLs.

17.31.26. Deve possuir homologação Anatel.

17.31.27. Deve possuir garantia do fabricante em regime 8x5BND de no mínimo 36 meses.

17.31.28. Deve ser licenciado o software de gestão de forma perpetua

17.31.29. Dever permitir o processo de HÁ ou seja configurar os equipamentos em modo FAIL OVER e LOAD BALANCE

17.2. LOTE ÚNICO - CONFIGURAÇÕES TÉCNICAS COMUNS MÍNIMAS DA SOLUÇÃO DE FIREWALL ANTISPAM E ANTIVÍRUS, COMO;:

17.2.1. Deve suportar armazenamento mínimo de 6 TB;

17... Deve permitir, pelo menos, a configuração e o gerenciamento de 800 domínios diferentes;

17.. Deve permitir, pelo menos, 700 políticas por recipiente por domínio;

17.32.1.4. Deve permitir, pelo menos, 2000 políticas por recipiente por sistema;

17.32.1.5. Deve permitir a configuração e uso de, pelo menos, 8CPUs virtuais;

17.32.1.6. Deve permitir a configuração e uso de, pelo menos, 32 GB de memória RAM;

17.32.1.7. Deve possuir a capacidade de roteamento de 500 (quinhetas) mil mensagens por hora efetuando recursos de antispam e antivírus de maneira simultânea;

17.32.1.8. Deve ser fornecido em virtual appliance;

17.32.1.9. Deve ser compatível e suportar a sua execução nos seguintes hypervisors: VMWareESXi, Microsoft Hyper-V, KVM e Citrix XenServer;

17.32.1.10. Deve ser capaz de funcionar como gateway SMTP para os servidores de correio existentes;

17.32.1.11. Deve ser capaz de funcionar como gateway, atuando como MTA (Mail Transfer Agent);

17.32.1.12. Deve ser capaz de operar em modo transparente, atuando como um proxy transparente para o envio de mensagens aos servidores de correio protegidos;

17.32.1.13. Deve poder ser instalado como um proxy SMTP transparente, para a análise do correio de saída;

17.32.1.14. Deve ser compatível com a implementação do protocolo WCCP para receber e-mail e analisar usando este protocolo;

17.32.1.15. A solução deve ter uma API baseada em REST disponível para fins de monitoramento, automação e orquestração;

17.32.2. Funcionalidades Gerais

17.32.2.1. A solução deve suportar listas de controles por usuários, por domínio e globalmente para todo o sistema;

17.32.2.2. A solução deve permitir a substituição, edição e personalização de mensagens de notificação de antivírus e anti-spyware;

17.32.2.3. A solução deve ser capaz de atrasar o envio de e-mail de grandes dimensões aos horários que são de menos carga;

17.32.2.4. A solução deve ser capaz de definir o encaminhamento de correio (relay) para um IP específico baseado no IP de origem da mensagem;

17.32.2.5. A solução deve fornecer suporte para múltiplos domínios de e-mail;

117.32.2.6. A solução deve suportar a implementação de políticas por destinatário, domínio, por tráfego de entrada ou de saída;

17.32.2.7. A solução deve ser capaz de entregar o correio baseado em usuários existentes em uma base LDAP;

17.32.2.8. A solução deve suportar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos. A quarentena deve ser acessada através de página Web e POP3;

17.32.2.9. A solução deve ser capaz de agendar o envio de relatórios de quarentena;

17.32.2.10. A solução deve ser capaz de realizar o armazenamento de e-mails (Archiving) baseado nas políticas de envio e recepção, com suporte também a armazenamento remoto;

17.32.2.11. A solução deve ser capaz de manter a filas de correio (Queue) em caso de falha na conexão de saída, atrasos ou erros de entrega;

17.32.2.12. A solução deve ser capaz de realizar a autenticação SMTP via LDAP, RADIUS, POP3 ou IMAP.

17.32.2.13. A solução deve ser capaz de manter listas de reputação do remetente com base em: quantidade de vírus enviados, quantidade de e-mails considerado spam, quantidade de destinatários equivocados;

17.32.2.14. A solução deve suportar direcionamento em IPv4 e IPv6;

17.32.2.15. A solução deve permitir o armazenamento de e-mail e quarentena localmente ou servidor remoto;

17.32.2.16. A solução deve possuir funcionalidades de Antispam, Antivírus, Anti-Spyware e Anti-Phishing;

17.32.2.17. A solução deve ser capaz de realizar a inspeção de correio da Internet de entrada e saída;

17.32.2.18. A solução deve possuir um assistente (Wizard) para o provisionamento fácil e rápido de configurações básicas e domínios para proteger;

17.32.2.19. A solução deve oferecer proteção contra ataques de negação de serviço como por exemplo Mail Bomb;

17.32.2.20. A solução deve fornecer controle de DNS reverso para proteção contra ataques de Anti-Spoofing;

17.32.3. Funcionalidades de Antispam

17.32.3.1. A solução deve se conectar em tempo real com a base de dados do fabricante para baixar atualizações Antispam;

17.32.3.2. A solução pode detectar se a origem de uma conexão é legal com base em um banco de dados de reputação de IP fornecido pelo fabricante;

17.32.3.3. A solução pode detectar se um e-mail é spam, verificando os URLs que contém, comparando-os com o banco de dados de reputação fornecido pelo fabricante;

17.32.3.4. A revisão de URLs deve permitir selecionar as categorias de URL que serão permitidas ou não, nos e-mails analisados. Este banco de dados de categorias

será atualizado pelo fabricante;

17.32.3.5. A solução deve ter novos mecanismos de detecção de SPAM, através da análise contínua do correio recebido e sua correlação posterior com eventos ocorridos em todo o mundo, permitindo assim definir e detectar novas regras de SPAM;

17.32.3.6. A solução deve ser capaz de realizar a análise heurística e definir limites máximos de acordo com o compartilhamento de mensagens e assim determinar se um e-mail é spam;

17.32.3.7. A solução deve ser capaz de realizar análise Bayesiana para determinar se um e-mail é spam;

17.32.3.8. A solução deve ser capaz de detectar se o e-mail é um boletim de informação (Newsletter);

17.32.3.9. A solução deve ter uma técnica que detecte o SPAM através do uso do Greylist, que classifica o correio com base em seu comportamento no início da sessão, como bloquear todos os e-mails e permitir apenas o encaminhamento. A solução deve ser capaz de filtrar e-mails baseados na URIs (UniformResourceIdentifier) contidos no corpo da mensagem;

17.32.3.10. A solução deve ser capaz de realizar análise com base em palavras proibidas (Banned Word);

17.32.3.11. A solução deve ter uma técnica que detecta SPAM através do uso de Greylist, que classifica o correio com base na sua entrada no início da sessão, como bloquear todos os e-mails e permitir apenas aqueles re enviados;

17.32.3.12. A solução permite criar listas de palavras;

17.32.3.13. A solução deve permitir o gerenciamento de spam com capacidade de aceitar, encaminhar (Relay) ,rejeitar (Reject) ou descartar (Discard);

17.32.3.14. A solução deve ser capaz de realizar análise de imagem e documentos PDF para a procura de spam;

17.32.3.15. A solução deve ser capaz de suportar listas de terceiros;

17.32.3.16. A solução deve suportar greylist para contas de e-mail em IPv4 e IPv6;

17.32.3.17. A solução deve ser capaz de detectar endereços IP forjados (Forged IP);

17.32.3.18. A solução permite identificar imagens que fazem referência ao conteúdo SPAM.

17.32.3.19. Ele deve suportar a análise das seguintes extensões GIF, JPEG, PNG;

17.32.3.20. aceleração da tecnologia de inspeção e bloqueia spam e malware de entrada e saída, garantindo que o email ou o domínio não seja comprometido ou entre na lista negra, visando proteger contra um remetente invalido via SMTP ou de um vírus de controle com um componente de spam, entregar a infraestrutura e reputação para que os canais de comunicação de e-mail permaneçam eficientes e com fluxo.

17.32.3.21. Dicionários personalizáveis e predefinidos incluindo padrões de expressões regulares, afim de evitar a perda acidental ou intencional de dados confidenciais ou regulamentados.

17.32.3.21. Detecção de vazamento, com a funcionalidade bloquear mensagens que contêm dados sensíveis ou executar arquivamento e criptografia de e-mail para auxiliar PCI DSS, HIPAA, GLB, e de conformidade SOX.

17.32.4. Funcionalidades de Controle de Sessão

17.32.4.1. A solução deve poder validar se o destinatário do e-mail recebido é uma caixa de correio válida;

17.32.4.2. A solução deve suportar SenderPolicy Framework (SPF);

17.32.4.3. A solução deve suportar Domain Keys Identified Mail (DKIM);

17.32.4.4. A solução deve suportar Domain BasedMessageAuthentication (DMARC);

17.32.4.5. A solução deve ser capaz de realizar uma inspecção profunda de cabeçalhos de e-mail;

17.32.5. Funcionalidades de Gerenciamento

17.32.5.1. A solução deve permitir sua configuração através de interface para acesso à Web (HTTP, HTTPS);

17.32.5.2. A solução deve ser capaz de permitir a criação de administradores exclusivos para a administração e configuração da solução por domínio, sendo também possível restringir o acesso por endereço IP e máscara de rede de origem;

17.32.5.3. A solução deve ser capaz de fornecer, pelo menos, dois níveis de acesso de gestão: Leitura/Gravação (Read/Write) ou somente leitura (ReadOnly);

17.32.5.4. A solução deve permitir a criação de perfis de configuração de forma granular, onde para cada perfil pode adicionar configurações específicas de funcionalidades como anti-spam, anti-vírus, autenticação, entre outros;

17.32.5.5. A solução deve suportar o fator de autenticação duplo para o login dos usuários de administrador;

17.32.6. Funcionalidades de HA

17.32.6.1. A solução deve permitir esquemas de Alta Disponibilidade, tanto Ativo-Ativo quanto Ativo-Passivo;

17.32.6.2. Quando a solução estiver implementada em alta disponibilidade, deve ser capaz de monitorar de status do link;

17.32.6.3. Quando a solução estiver implementada em alta disponibilidade, deve suportar o Failover de rede;

17.32.6.4. Quando a solução estiver implementada em alta disponibilidade, deve ser capaz de sincronizar as mensagens de quarentena de e-mails;

17.32.6.5. Quando a solução estiver implementada em alta disponibilidade Ativo/Passivo, deve ser possível sincronizado os dados de mensagens de e-mails e configurações;

17.32.6.6. Quando a solução estiver implementada em alta disponibilidade, deve ser capaz de detectar e notificar a falha de algum dispositivo;

17.32.6.7. O modo Ativo-Passivo deve suportar até 2 membros no cluster;

17.32.7. Funcionalidades de Anti-Malware

17.32.7.1. A solução deve ter a capacidade de avaliar, reter e / ou bloquear e-mails que têm ameaças avançadas, Dia zero, através de envio para análise em solução de sandbox externa e do mesmo fabricante;

17.32.7.2. A solução deve ser capaz de filtrar anexos e conteúdo de e-mails;

17.32.7.3. A solução deve ser capaz de executar análise de antivírus/antispyware em arquivos compactados como ZIP, PKZIP, LHA, ARJ e RAR;

17.32.7.4. A solução deve ter uma base de informações de malware fornecida pelo fabricante e terceiros aliados, que podem ser atualizados de forma recorrente;

17.32.7.5. Após a detecção de um malware, a solução pode executar as seguintes ações: envie uma mensagem de notificação, reenviar mensagens e malwares para uma conta definida, reescreva o destinatário;

17.32.7.6. A solução deve ser capaz de verificar os e-mails que são liberados da quarentena SPAM pelo usuário em busca de conteúdo malicioso;

17.32.8. Funcionalidades de Virus Outbreak

17.32.8.1. A solução deve ter um banco de dados de malware baseado em técnicas de sanboxing. Este banco de dados deve ser fornecido pelo fabricante da solução enquanto durar a garantia/licenciamento da solução;

17.32.8.2. A solução deve ser capaz de analisar as imagens em busca de tipos inadequados de imagens com conteúdo para adultos;

17.32.9. Funcionalidades de DLP

17.32.9.1. Deve ser fornecido também uma solução de DLP, para detectar informações sensíveis que podem estar vindo através de e-mail;

17.32.9.2. A funcionalidade de DLP deve permitir especificar a informação a ser detectada como palavras, frases e expressões regulares;

17.32.9.3. A funcionalidade de DLP deve possuir uma lista predefinida de tipos de informações, como números de cartão de crédito e outros;

17.32.9.4. A funcionalidade de DLP deve permitir a criação e armazenamento de impressões digitais (Fingerprint) de documentos;

17.32.9.4. A funcionalidade de DLP deve permitir a criação de filtros por arquivo;

17.32.9.6. A funcionalidade de DLP deve permitir a geração e armazenamento de impressões digitais (Fingerprint) de anexos em e-mail;

17.32.9.7. A funcionalidade de DLP deve permitir o armazenamento de impressões digitais (Fingerprints) para arquivos antigos e também para novos arquivos que foram atualizados;

17.32.10. Criptografia

17.32.10.1. A solução deve suportar criptografia da mensagem baseada em identidade (IdentityBasedEncryption IBE) para que o destinatário não requeira uma PSK ou certificado instalado anteriormente para a de criptografado;

17.32.10.2. Criptografia de mensagens com IBE, deve suportar tanto o método push e pull, em que a mensagem criptografada é armazenada na plataforma de e-mail para acesso remoto autenticado ou ser enviado como anexo para o destinatário;

17.32.10.2. Em ambos métodos da criptografia IBE, deve ter um registro do usuário do destino na plataforma de e-mail, de modo que, para ver as mensagens criptografadas, um processo de autenticação é necessário;

17.32.10.4. Deve suportar criptografia de e-mail usando S / MIME;

17.32.10.5. Deve suportar SMTPS e SMTP over TLS;

17.32.11. Conformidade

17.32.11.1. A solução deve analisar o conteúdo e anexos de uma mensagem em busca de palavras que indicam que o correio deve ser em quarentena, criptografado, arquivado, bloqueado, marcado, substituído ou encaminhado para outro host;

17.32.11.2. Deve ter dicionários predefinidos que estejam em conformidade com regulamentos como HIPAA, GLB, SOX, esses dicionários devem identificar: SIN canadense, US SSN, cartão de crédito, ABA Routing, CUSIP, ISIN e poder definir dicionários personalizados;

17.32.11.3. Você deve inspecionar arquivos protegidos por senha, usando senhas predefinidas, uma lista de senhas ou pesquisar a palavra senha no corpo;

17.32.12. Desarmar e Reconstruir

17.32.12.1. Deve prover a opção de remover ou neutralizar conteúdos potencialmente maliciosos e reconstruí-lo mais tarde. Por exemplo, em arquivos como o MSOffice e pdf que possuem macros, java ou HTML com URLs mal-intencionados;

17.32.13. Funcionalidades de Log e Relatórios

17.32.13.1. A solução deve ser capaz de armazenar logs e eventos localmente e também enviá-los para solução de análise de logs ou servidores remotos (Syslog);

17.32.13.2. A solução deve permitir o relato de atividade, analisando os arquivos de eventos (logs) e apresentá-los na tabela ou formato gráfico;

17.32.13.3. A solução deve permitir gerar relatórios sob demanda ou programados em intervalos de tempo específicos;

17.32.13.4. A solução deve permitir gerar e enviar relatórios em formato PDF ou HTML;

RFCs suportadas requeridas

17.32.13.5. Deve implementar as seguintes RFC’s: RFC 1213, RFC 1918, RFC 1985, RFC 2034,

RFC 2045, RFC 2505, RFC 2634, RFC 2920, RFC 3207, RFC 3461, RFC 3463, RFC 3464, RFC 3635, RFC 4954, RFC 5321, RFC 5322, RFC 6376, RFC 6522, RFC 6409, RFC 7208, RFC 2088, RFC 2177, RFC 2221, RFC 2342, RFC 2683, RFC 2971, RFC 3348, RFC 3501, RFC 3502, RFC 3516, RFC 3691, RFC 4315, RFC 4469, RFC 4731, RFC 4959, RFC 5032, RFC 5161, RFC 5182, RFC 5255, RFC 5256, RFC 5258, RFC 5267, RFC 5819, RFC 6154, RFC 6851, RFC 7162, RFC 1939, RFC 2449, RFC 1155, RFC 1157, RFC 1213, RFC 2578, RFC 2579, RFC 2595, RFC 3410, RFC 3416;

17.32.14.1. Licenciamento e Garantia da Solução

17.32.14.1. Deverá possuir licenciamento de todos os recursos listados nas especificações técnicas por, pelo menos, 60 (sessenta) meses;

17.32.14.2. A solução deve estar completamente licenciada para tratamento de mensagens de entrada e saída para, pelo menos, 50.000 (cinquenta mil) caixas postais de e-mail;

17.32.14.3. A garantia e suporte exigidos deverão ser de, pelo menos, 60 (sessenta) meses;

17.32.14.1. A garantia e suporte deverão ser prestados diretamente pelo fabricante dos produtos;

17.32.14.4. O fabricante deverá oferecer possibilidade de abrir chamados técnicos por telefone ou Internet;

17.32.14.5. Os chamados técnicos deverão ser abertos diretamente no fabricante dos produtos e gerenciados pelo menos, prioritariamente via internet ou através de número telefônico 0800 ou equivalente à ligação gratuita, fornecendo neste momento o número, data e hora de abertura do chamado.

17.32.14.6. As novas versões, release, atualizações e correções dos softwares e firmwares dos hardwares adquiridos, deverão ser disponibilizados ao ITEC, sem ônus durante o período de garantia;

17.32.14.7. A cobertura do atendimento deverá ser 24 x 7;

Atesto, sob a minha responsabilidade, que o conteúdo do Termo de Referência se limita ao mínimo imprescindível à satisfação do interesse público, presente na generalidade dos produtos e modelos existentes no mercado, não consignando marca ou característica, especificação ou exigência exclusiva, excessiva, impertinente, irrelevante ou desnecessária que possa direcionar o certame ou limitar ou frustrar a competição ou a realização do objeto contratual.

Maceió, 10 de dezembro de 2021.

José Álvaro de Oliveira	Raymundo Sampaio Fernandes Coutinho	Paulo Silva
Gerente de operações – ITEC	Gerente de Projetos - ITEC	Gerente de desenvolvimento - ITEC
Matrícula nº 53.231-2	Matrícula 033-7	Matrícula 052-3

ANEXO I

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Pelo presente instrumento e na melhor forma de direito, de um lado XXX (NOME), NACIONALIDADE), (ESTADO CIVIL), lotado no Departamento XXXXX, do ITEC XXXXXX, e de outro (NOME), (NACIONALIDADE), (ESTADO CIVIL) ou *nome e qualificação do ITEC*, residente e domiciliado na (ENDEREÇO)

Considerando que para bom e fiel desempenho das atividades do ITEC faz-se necessária a disponibilização de informações técnicas e confidenciais, incluídas as de projeto, especificação, funcionamento, organização e desempenho da referida ITEC.

CLÁUSULA PRIMEIRA – DO OBJETO

O objeto do presente termo é a proteção das INFORMAÇÕES CONFIDENCIAIS disponibilizadas pelo ITEC, em razão da relação de emprego desenvolvida pelas partes.

CLÁUSULA SEGUNDA – DAS DEFINIÇÕES

Todas as informações técnicas obtidas através da relação de serviço com o ITEC e relacionadas a projeto, especificação, funcionamento, organização ou desempenho

da referida função serão tidas como CONFIDENCIAIS E SIGILOSAS.

PARÁGRAFO ÚNICO: Serão consideradas para efeito deste termo toda e qualquer informação, patenteada ou não, de natureza técnica, operacional, comercial, jurídica, Know-how, invenções, processos, fórmulas e designs, patenteáveis ou não, sistemas de produção, logística e layouts, planos de negócios (*business plans*), métodos de contabilidade, técnicas e experiências acumuladas, documentos, contratos, papéis, estudos, pareceres e pesquisas a que o funcionário tenha acesso:

a) por qualquer meio físico (*v.g.* documentos expressos, manuscritos, fac-símile, mensagens eletrônicas (e-mail), fotografias etc;

b) por qualquer forma registrada em mídia eletrônica (fitas, cd´s, dvd´s, disquetes etc);

c) oralmente.

CLÁUSULA TERCEIRA – DA RESPONSABILIDADE

O colaborador, prestador de serviço, comissionados e os efetivos em cargo ou não de confiança, compromete-se a manter sigilo não utilizando tais informações confidenciais em proveito próprio ou alheio.

PARÁGRAFO PRIMEIRO: As informações confidenciais confiadas aos colaboradores somente poderão ser abertas a terceiro mediante consentimento prévio e por escrito do ITEC, ou em caso de determinação judicial, hipótese em que o empregado deverá informar de imediato, por escrito, à ITEC para que esta procure obstar e afastar a obrigação de revelar as informações.

CLÁUSULA QUARTA – DAS INFORMAÇÕES NÃO CONFIDENICAIS

Não configuram informações confidenciais aquelas:

a) já disponíveis ao público em geral sem culpa do funcionário;

b) que já eram do conhecimento do funcionário antes de sua do ingresso no ITEC e que não foram adquiridas direta ou indiretamente do ITEC;

c) que não são mais tratadas como confidenciais pelo ITEC.

CLÁUSULA QUINTA – DA GUARDA DAS INFORMAÇÕES

Todas as informações de confidencialidade e sigilo previstas neste termo terão validade durante toda a vigência deste instrumento, enquanto perdurar a relação de trabalho e, ainda, por um período mínimo de 01 (um) ano do rompimento do vínculo do funcionário com a ITEC.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES

Deverá o funcionário:

I) usar tais informações apenas com o propósito de bem e fiel cumprir os fins do ITEC;

II) manter o sigilo relativo ás informações confidenciais e revelá-las apenas aos colaborador que tiverem necessidade de ter conhecimento sobre elas;

III) proteger as informações confidenciais que lhe foram divulgadas, usando o mesmo grau de cuidado utilizado para proteger suas próprias informações confidenciais;

IV) manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou informações confidenciais, devendo comunicar à ITEC, imediatamente, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade.

PARÁGRAFO PRIMEIRO: O funcionário fica desde já proibido de produzir cópias ou *backup*, por qualquer meio ou forma, de qualquer dos documentos a ele fornecidos ou documentos que tenham chegado ao seu conhecimento em virtude da relação de emprego.

PARÁGRAFO SEGUNDO: O funcionário deverá devolver, íntegros e integralmente, todos os documentos a ele fornecidos, inclusive as cópias porventura necessárias, na data estipulada pelo ITEC para entrega, ou quando não for mais necessária a manutenção das informações confidenciais, comprometendo-se a não reter quaisquer reproduções, cópias ou segundas vias, sob pena de incorrer nas responsabilidades previstas neste instrumento.

PARÁGRAFO TERCEIRO: O funcionário deverá destruir todo e qualquer documento por ele produzido que contenha informações confidenciais do ITEC, quando não mais for necessária a manutenção dessas informações confidenciais, comprometendo-se a não reter quaisquer reproduções, sob pena de incorrer nas responsabilidades previstas neste instrumento.

CLÁUSULA SÉTIMA – DAS DISPOSIÇÕES ESPECIAIS

Ao assinar o presente instrumento, o funcionário manifesta sua concordância no seguinte sentido:

I) todas as condições, termos e obrigações ora constituídas serão regidas pelo presente Termo, bem como pela legislação e regulamentação brasileiras pertinentes;

II) o presente termo só poderá ser alterado mediante a celebração de novo termo, posterior e aditivo;

III) as alterações do número, natureza e quantidade das informações confidenciais disponibilizadas pelo ITEC não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Confidencialidade e Sigilo, que permanecerá válido e com todos os seus efeitos legais em qualquer das situações tipificadas neste instrumento;

IV) o acréscimo, complementação, substituição ou esclarecimento de qualquer das informações confidenciais disponibilizadas para o funcionário, em razão do presente objetivo, serão incorporadas a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, não sendo necessário, nessas hipóteses, a assinatura ou formalização de Termo aditivo.

CLÁUSULA OITAVA – DA VALIDADE

Este termo tornar-se-á válido a partir da data de sua efetiva assinatura pelas partes.

Parágrafo Único: As disposições deste instrumento devem, contudo, ser aplicadas retroativamente a qualquer informação confidencial que possa já ter sido divulgada, antes da data de sua assinatura.

CLÁUSULA NONA – DAS PENALIDADES

A não-observância de quaisquer das disposições de confidencialidade estabelecidas neste instrumento, sujeitará ao funcionário infrator, como também ao agente causador ou facilitador, por ação ou omissão de qualquer daqueles relacionados neste Termo, ao pagamento, ou recomposição, de todas as perdas e danos comprovadas pelo ITEC, bem como as de responsabilidade civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

CLÁUSULA DÉCIMA – DO FORO

O foro competente para dirimir quaisquer dúvidas ou controvérsias resultantes da

execução deste Instrumento é o da cidade de Xxxxxxx, Estado Xxxxxxxx, caso não sejam solucionadas administrativamente.

E por estarem assim justas e acordadas, as Partes assinam o presente Termo em 02 (duas) vias de igual teor e forma, na presença de duas testemunhas.

Cidade, de de Ano .

_____

Contratada

_____

ITEC / Funcionário

TESTEMUNHAS:

Nome: _____

CPF:

Nome: _____

CPF:

ANEXO II

TERMO DE CIÊNCIA DAS REGRAS DE SEGURANÇA

Por meio deste instrumento, xxxxxx, nacionalidade xxxx, cargo xxxx, carteira de identidade nº xxxx, expedida por xxxxx, CPF xxxxx, declaro estar ciente e concordo com o inteiro teor das normas estabelecidas no Termo de compromisso, sigilo e confidencialidade.

Por fim, declaro que concordo e aceito o teor deste termo e das normas a que faz referência, bem como que tenho acesso a cópias dos documentos aqui mencionados.

Maceió, _____ de _____, 20____

_____

Documento assinado eletronicamente por **José Álvaro de Oliveira**, **Gerente** em 06/01/2022, às 14:13, conforme horário oficial de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.al.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **10084337** e o código CRC **65837BF2**.

Processo nº E:41506.0000000507/2021	Revisão 08 SEI ALAGOAS	SEI nº do Documento 10084337