**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° (41506.00000000037/2022)**

## 1. DO OBJETO

**1.1.** A presente solicitação tem por objetivo para aquisição de SOLUÇÃO DE SISTEMA DE MONITORAÇÃO PARA CIBERSEGURANÇA , incluindo licenciamento, suporte técnico 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:

| Item | Catmat/ catser | Descrição | Unidade de Medida | Quantidade |
|---|---|---|---|---|
| 01 | 481647 | Sistema de monitoração para cibersegurança (de grande porte, com redundância), incluindo suporte técnico, licenciamento e garantia. | UND | 01 |

**1.2.** A presente contratação terá vigência de 03(três) 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.

**1.3.** 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.

**1.3.1.** Todos os equipamentos no que diz respeito a licenças de uso de software de forma perpetua, devem ter garantia de 36 (trinta e seis) 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.

**1.3.2.** 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).

**1.4.** 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.

## 2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

**2.1.** 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.

**2.2.** 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.

**2.3.** 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.

**2.4.** 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, se identificará rapidamente as ameaças infiltradas na rede, onde podemos decidir que parte do trafego, deve ser analisado em tempo real sobre os fluxos de dados complexos, que reduzirá os gargalos operacionais. De

modo que, combatam as ameaças cibernéticas mais avançadas, detectando fraudes e mantendo as comunicações seguras para todos.

**2.5.** 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.

**2.6.** Insto salientar, dá importância da solução pretendida, que nos possibilitará uma segurança mais ampla para toda a rede, com uma vigilância 24 horas por dia, 07 dias da semana. Onde será realizado um monitoramento completo da infraestrutura estatal, que nos possibilitará a detecção de ataques sofisticados em tempo real, com respostas imediata e precisa, nos possibilitando o respaldo para a correção de falhas e na recuperação de evidências da investigação do evento. Aliados ao restabelecimento das operações a normalidade de forma ágil, em conjunto com a implementação de melhorias na segurança pós-acidente, com o mínimo impacto aos usuários finais.

**2.7.** Em reforço ao item 1.1 (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.

**2.8.** 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.

**2.9.** A presente aquisição é imprescindível para garantir alto desempenho e segurança 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.

**2.10.** 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.

**2.11.** A aquisição das soluções de segurança de rede possibilitará qualificar a administração de TI, tornando-a efetivamente comprometida com a qualidade dos serviços a serem disponibilizados para todo o Estado, com excelência de gestão e, principalmente com as áreas fins do Instituto de Tecnologia em Informática e Informação de Alagoas - ITEC.

**2.12.** 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.

**2.13.** 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.

**2.14.** 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.

**2.15.**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.

**2.16.** Saliento dá gravidade, aos últimos eventos ocorridos no Brasil, a exemplo das invasões aos sites e sistemas do **MINISTÉRIO DA JUSTIÇA, MINISTÉRIO DA SAÚDE** e demais órgão da esfera federal, sem mencionar ainda, alguns órgãos da esfera estadual, fato a pouco ocorrido, a exemplo do **GOVERNO DO ESTADO DA BAHIA,** que ficaram horas fora do ar, além da exposição sofrida de dados sigilosos de milhões de brasileiros.

**2.17.** Ilustro a importância desta solução, que vem a preencher uma lacuna no que cerne a fermentas de analise, detecção e proteção do ambiente de rede, e não só para o DATACENTER DO GOVERNO DO ESTADO DE ALAGOAS, mas bem como para a análise de 360º (TREZENTOS E SESSENTA GRAUS), de possíveis e invariáveis ameaças cibernéticas a todos do ente público governamental. Onde, esta solicitação dar-se-á uma vez que, o prejuízo em caso de vazamento de dados se tornará imensurável, se comparado ao valor desta solução pretendida, que evitará desta forma o desgaste da imagem do ITEC, bem como auxiliando-nos na prevenção de possíveis ações judiciais, e possíveis multas, por ineficiência da segurança da rede.

**2.18.**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. CLASSIFICAÇÃO DOS BENS COMUNS

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

## 4. DOS DOCUMENTOS DE HABILITAÇÃO

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

**4.1.1.** 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. 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.** Características: fornecimento de todos os componentes da solução de sistema de monitoração para cibersegurança, incluindo licenciamento, suporte técnico e garantia da solução, 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.

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

**5.1.3.3 .** 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.

## 5. DA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

**5.1.** 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.

**5.1.1.** 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.

**5.2.** 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.

**5.3.** 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.

**5.4.** 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.

**5.5.** 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.

**5.6.** 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.

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

**5.8.** 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.

## 6.0. OBRIGAÇÕES DA CONTRATANTE

**6.1.** São obrigações da contratante:

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

**6.1.2.** 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;

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

**6.1.4.** Acompanhar e fiscalizar o cumprimento das obrigações da contratada,

através de comissão/servidor especialmente designado;

**6.1.5.** Efetuar o pagamento à contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

**6.2.** 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.

## 7. OBRIGAÇÕES DA CONTRATADA

**7.1.** 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:

**7.1.1.** 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;

**7.1.1.1.** 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;

**7.1.2.** 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);

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

**7.1.4.** 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;

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

**7.1.6.** 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;

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

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

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

## 8. SUBCONTRATAÇÃO

**8.1.** Não será admitida a subcontratação do objeto licitatório.

## 9.0. ALTERAÇÃO SUBJETIVA

**9.1.** 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.

## 10. DO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

**10.1.** 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.

**10.1.1.** 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.

**10.2.** 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.

**10.2.1.** 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.

**10.2.2.** 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.

**10.3.** 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.

## 11. DO PAGAMENTO

**11.1.** 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.

**11.1.1.** 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.

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

**11.3.** 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.

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

**11.5.** 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.

**11.5.1.** 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.

**11.6.** 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.

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

**11.7.** 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.

**11.8.** 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.

**11.9.** 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.

**11.9.1.** 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.

**11.10.** 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.

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

**11.11.1.** 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.

## 12. DO REAJUSTE

**12.1.** Os preços são fixos e irreajustáveis.

**12.2.** 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.

## 13. DA GARANTIA DE EXECUÇÃO

**13.1.** Não haverá exigência de garantia de execução para a contratação.

## 14. DAS SANÇÕES ADMINISTRATIVAS

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

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

**14.1.2.** Não entregar a documentação exigida no edital;

**14.1.3.** Apresentar documentação falsa;

**14.1.4.** Causar o atraso na execução do objeto;

**14.1.5.** Não mantiver a proposta;

**14.1.6.** Falhar na execução do contrato;

**14.1.7.** Fraudar a execução do contrato;

**14.1.8**. Comportar-se de modo inidôneo;

**14.1.9.** Declarar informações falsas; e

**14.1.10.** Cometer fraude fiscal.

**14.2**. As sanções do subitem 14.1. 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.

**14.3.** 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:

**14.3.1.** 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

**14.3.2.** Multa.

**14.4**. 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.

**14.5.** 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.

**14.5.1.** 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.

**14.6.** 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.

**14.7.** 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.

**14.8.** 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.

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

## 15. DAS ESPECIFICAÇÕES TÉCNICAS E FUNCIONALIDADES PARA A SOLUÇÃO DE SISTEMA DE MONITORAÇÃO PARA CIBERSEGURANÇA (Appliance Físico).

**15.1.** Conjunto de appliances com 1 (hum) WDC e 3 (três) WDA – soman do quatro appliances distintos - com capacidade para analisar até 6Gbps (seis gigabits por segundo) de tráfego, utilizando placa de captura especializada com 2 portas 10GbE. Conta com todas as funcionalidades licenciadas perpetuamente e subscrição de Threat Intelligence durante o período de contrato. Possui capacidade internade armazenamento de 105TB para PCAPs e 90TB para meta dados/logs/flows, em drives NVMe. Esse sistema permite a operação em alta-disponibilidade para acesso aos dados de meta dados/logs/flows

### 15.2. Especificação técnicas

**15.2.1.** Realizar análises, aprendizado de máquina e detecções de eventos de segurança a nível de rede e aplicações (camada 7);

a) HTTP 1.0 e 1.1;

b) Apache JServProtocol (AJP);

c) Domain Name System (DNS);

d) Oracle Transparent Network Substrate (TNS);

e) PostgreSQL (pgsql);

f) MySQL.

**15.2.2.** Tabular Data Stream (TDS);

**15.2.3.** Server MessageBlock (SMB), nas versões 1 e 2;

a) TransportLayer Security (TLS), nas versões 1.0, 1.1 e 1.2;

b) Simple Mail TransferProtocol (SMTP);

c) LightweightDirectory Access Protocol;

**15.2.4.** Instalação em appliance, com hardware e software integrados pelo fabricante;

**15.2.4.1.** Deve extrair informações a partir da rede, de forma passiva, em portas espelhadas em switches (ex. SPAN, RSPAN) ou com a utilização de dispositivos passivos (TAPs). Não serão aceitas soluções intrusivas, que requeiram a instalação de softwares em servidores ou que atuem de forma ativa na rede;

**15.2.4.2.** Extrair metadados de requisições e respostas de todas as transações

analisadas, inclusive lentas e/ou com erros, efetuadas nos protocolos suportados, exportando os detalhes de cada transação executada, de forma granular (sem sumarizar/agregar);

**15.2.4.3.** Reconstruir o conteúdo (body HTML) de requisições e respostas em protocolos HTTP e AJP;

**15.2.5.** Deve calcular métricas de performance de cada transação coletada, informando:

a)Tempo para abertura da conexão TCP;

b) Tempo para execução da requisição pelo cliente, após início da conexão TCP;

c) Tempo para resposta da requisição pelo servidor;

d) Tempo para transmissão dos dados da resposta;

e) Quantidade de retransmissões TCP (pelo cliente e pelo servidor);

f) Quantidade de pacotes Zero Window (pelo cliente e pelo servidor).

**15.2.6.** Todos os dados extraídos pelo appliance devem ser estruturados em formato JSON ou XML e transmitidos utilizando protocolo de mensageria;

a) reconstrução das transações/eventos nos protocolos suportados deve ser executada em tempo real. Não serão aceitas soluções que primeiro armazenam os dados (em PCAP ou qualquer outro formato de armazenamento de pacotes de rede) e depois executam a extração de metadados;

b) Executar DeepPacketInspection (DPI) em todo tráfego que chega às interfaces de coleta, identificando aplicações através de assinaturas. O DPI deve identificar as seguintes aplicações automaticamente: FTP, POP, SMTP, IMAP, DNS, HTTP, NFS, SMB, PostgreSQL, MySQL, Oracle (SGBD), MS SQL, RTSP, GRE, SSH, HTTPS, HTTP Proxy, SIP, VNC, Telnet, RDP, Websocket, Bittorrent, Youtube, Skype, Whatsapp. Não serão aceitas soluções que identificam aplicações apenas a partir do número da porta TCP/UDP;

c) Possuir 4 (quatro) portas exclusivas e dedicadas para coleta de dados, em interfaces Gigabit Ethernet, utilizando placa aceleradora com 4GB de RAM integrada. Deve executar em hardware a marcação de timestamp nos pacotes coletados e a sincronização de tempo com placas similares, com precisão de microssegundos;

d) Possuir 2 (duas) portas Ethernet 10GBase-T RJ45, capazes de receber tráfego espelhado via túnel GRE (GenericRoutingEncapsulation), proveniente de espelhamento remoto (ex: ERSPAN), extraindo em tempo real metadados de eventos contidos no túnel;

e) Possuir porta Gigabit Ethernet RJ45 dedicada para serviço Intelligent Platform Management Interface (IPMI);

f) Permitir configuração de bloqueio de pacotes nas interfaces de coleta, utilizando informações de IP e portas TCP/UDP;

**15.2.7.** Fazer a coleta contínua de fluxos e pacotes completos, em formato PCAP. Esses dados devem ser relacionados em interface com os demais metadados extraídos dos protocolos de rede em camada de aplicação, permitindo assim filtrar os dados que serão analisados por flow ou transação de rede;

a) Prover capacidade de armazenamento de 100TB (cemterabytes), em drives NVMe, exclusivos para armazenamento de arquivos PCAP;

b) Deve licenciar funcionalidade integrada para reconstrução completa de arquivos, a partir dos PCAPs capturados, inclusive de arquivos anexos a e-mails, trafegados na

web ou compartilhados entre usuários.

**15.3. Performance:**

**15.3.1.** Deve suportar a análise de tráfego Ethernet com throughput contínuo de 6 (seis) Gigabits por segundo, sem perda de pacotes;

**15.3.2.** Caso se julgue necessário, a performance do sistema deverá ser comprovada em demonstração executada no laboratório do fabricante, no prazo máximo de 15 dias, utilizando equipamento similar ao ofertado. Não serão aceitos equipamentos que deixem de atender a qualquer requisito de performance.

a) Permitir a procura em transações e eventos armazenados, através de filtro textual. O sistema deve indexar as informações coletadas;

b) Prover capacidade de armazenamento de 90TB (noventaTerabytes) brutos, em drives NVMe, dedicados para armazenamento de metadados provenientes da rede e logs;

**15.3.2.1.** Deve contemplar todo o processo de instalação e atualização, incluindo serviços e equipamentos, a ser realizado nas dependências do Contratante somente por profissionais autorizados pelo fabricante da solução;

**15.3.2.2.** Todos os equipamentos instalados deverão ser homologados pelo fabricante original da solução;

**15.3.2.3.** As versões de firmwares e softwares instaladas deverão estar de acordo com os termos de garantia do fabricante;

**15.3.2.4.** Permitir a criação de dashboards customizados, contendo apenas gráficos e tabelas escolhidas pelo usuário;

**15.3.2.5.** Permitir a criação de alarmes customizados pelo usuário, utilizando qualquer metadado armazenado como parâmetro para envio de alertas;

**15.3.2.6.** Permitir o envio dos alertas para sistema de SIEM, utilizando formato CEF (Common Evento Format);

**15.3.2.7.** Possuir interface web em HTML5;

**15.3.2.8.** Utilizar técnicas de Machine Learning ou similares para identificar não apenas ataques amplamente divulgados, mas também ataques novos ou desconhecidos (zero day);

**15.3.3.** Aprender os comportamentos de usuários e dispositivos de rede para identificar anomalias que possam estar envolvidas em ataques:

a) O aprendizado deve ser supervisionado, permitindo ao administrador do sistema confirmar ou rejeitar eventuais comportamentos, com posterior inclusão de tal classificação no aprendizado.

**15.3.4.** Detectar, pelo menos, as seguintes atividades maliciosas:

a) Acesso a endereços IP e URLs conhecidamente maliciosas;

b) As informações sobre a reputação dos recursos acessados devem ser fornecidas por entidades especializadas em inteligência;

c) Acessos a aplicações realizados por mecanismos automatizados (bots).

**15.3.5.** Inundações de pacotes (floods);

**15.3.6.** Ataques a usuários e senhas de aplicações mediante tentativas sucessivas (brute force anddictionaryattacks);

**15.3.7.** Varreduras de redes para mapeamento de ativos e descoberta de

vulnerabilidades;

**15.3.8.** Anomalias em comportamentos de usuários da rede interna para identificação de InsiderThreats;

**15.3.9.** Injeções de comandos em aplicações;

**15.3.10.** Movimento Lateral.

**15.3.11.** Na ocorrência de eventos detectados com características de ataques, alertas devem ser produzidos com informações de contexto, comportamento e assinaturas pertinentes à detecção;

**15.3.12.** Monitorar o status de risco de segurança e computar reputação de usuários e endpoints IP, incluindo os seguintes tipos de dispositivos:

a) Estações de trabalho;

b) Impressoras;

c) Servidores de aplicação;

d) Banco de dados;

e) Servidores DNS;

f) Dispositivos IOT;

g) Celulares;

h) Sistemas de armazenamento;

i) Sistemas de autenticação, autorização (AAA) e acesso (IAM) à rede;

**15.3.13.** Deve incluir subscrição (assinatura a serviço) de API de ameaças conhecidas (ThreatIntelligence), totalmente compatível com o sistema ofertado, permitindo acesso durante o período do contrato de suporte/garantia às seguintes informações:

a) Lista de endereços IP identificados como maliciosos;

b) Lista de URL (UniformResourceLocator) classificadas como maliciosas;

c) Classificação de conteúdo de serviços Web;

d) Listas de hashes MD5 de arquivos classificados como maliciosos;

**15.3.14.** Modelo de Machine Learning treinado especificamente para detecção de Malwares.

a) O algoritmo de detecção de Malware deve permitir a análise de pelo menos cinco mil arquivos por minuto, através da análise do conteúdo do arquivo (sem a necessidade de utilização de sandbox);

b) Esse módulo deverá ser executado localmente, sem necessidade do envio de arquivos para nuvem.

**15.3.15.** A lista com classificação de reputação de serviços Web deve conter pelo menos 25 (vinte cinco) bilhões de URLs;

**15.3.16.** As informações providas devem ser atualizadas dinamicamente, à medida que novas ameaças são detectadas na Internet;

**15.3.17.** O acesso aos dados da subscrição deve ser feito via HTTP REST API, de forma totalmente integrada e orquestrada pelo sistema, para correlação automatizada de metadados com as bases de ameaças conhecidas;

**15.3.18.** Deve fornecer informações de Whois e Geolocalização para os endereços

IP e URL classificadas como ameaças;

**15.3.19.** A API deve fornecer o histórico de ameaça de um determinado endereço IP;

**15.3.20.** As informações sobre endereços IP devem incluir quais tipos de ameaças foram identificadas, com pelo menos as seguintes classificações: exploits, phishing, botnet, DoS, scanners de portas, proxies anônimos e origens de spam;

**15.3.21.** O provedor desses serviços deve possuir ciclo contínuo de tratamento das informações, utilizando fontes de detecção espalhadas por todo o mundo.

**15.4. SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA**

**15.4.1.** Tem por objetivo analisar eventos, orientar a resposta e documentar os incidentes de segurança da informação. Tal serviço deverá ser executado obedecendo aos frameworks do NIST (Nationall nstitute of Standards and Technology) e SANS Institute para resposta a incidente de segurança da informação;

**15.4.2.** As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das tácticas e técnicas de ataque para que, por meio da atuação conjunta (PURPLE TEAM), aumente-se a efetividade da proteção do ambiente;

**15.4.3.** Um incidente de segurança é definido como qualquer evento adverso em sistemas computacionais, feito de forma intencional ou acidental, levando a violação de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade;

**15.4.4.** O início do processo de resposta a incidente de segurança se dará das seguintes formas:

a) Sempre que um evento adverso for submetido à Contratada, pelo corpo técnico da Contratante, a qualquer tempo;

b) A partir de consultas diárias ao Sistema de monitoração para cibersegurança, deve identificar situações onde endpoints IP, sistemas ou usuários apresentem comportamentos comprovadamente ou potencialmente nocivos a segurança dos dados.

**15.4.5.** Após o incidente de segurança ser aberto, será de responsabilidade do grupo de resposta a incidente de segurança (Blue Team) da Contratada, analisar os logs, pacotes, flows e demais artefatos coletados, a fim de no primeiro instante identificar do que se trata o incidente e avaliar o risco do mesmo;

**15.4.6.** Uma vez realizadas as análises iniciais do incidente, o grupo de resposta a incidente de segurança (Blue Team) da Contratada, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do Contratante;

**15.4.7.** Como próximo passo o grupo de resposta a incidente de segurança (Blue Team) da Contratada, deverá comunicar ao time de segurança da informação do Contratante as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente;

**15.4.8.** A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente;

**15.4.9.** Após análises iniciais do incidente, caberá ao grupo de resposta a incidente

de segurança (Blue Team), realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e todos os seus artefatos coletados;

**15.4.10.** Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança (Blue Team) da Contratada, deverá definir uma estratégia para a mitigação e contenção do ataque em questão;

**15.4.11.** Ao longo do processo de resposta ao incidente de segurança, a Contratada através do grupo de resposta a incidente de segurança (Blue Team), deve documentar toda e quaisquer evidências e identificação dos serviços e usuários envolvidos. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

**15.4.12.** A análise deve ser realizada com o objetivo de identificar pessoas, locais e/ou eventos relacionados, correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão;

**15.4.13.** Caso seja necessária a reconstrução do ataque, este deve ser realizado pela Contratada em ambiente controlado, usando-se, por exemplo, de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da Contratada;

**15.4.14.** O grupo de resposta a incidente de segurança (Blue Team) da Contratada, deve documentar as lições aprendidas no incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos;

**15.4.15.** O serviço de resposta a incidentes será responsável por monitorar, configurar e operar o Sistema de monitoração para cibersegurança, visando a análise de logs, flows e pacotes de rede;

**15.4.16.** O regime de execução deste serviço deverá ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);

**15.4.17.** A Contratada irá prover inteligência de proteção contra ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra ataques cibernéticos, sendo responsável por:

a) Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela Contratada;

b) Criar e revisar periodicamente regras (casos de uso) para detecção de ataques no Sistema de monitoração para cibersegurança, realizando as adaptações e evoluções necessárias;

c) Implementar procedimentos para triagem de alertas e resposta a incidentes.

### 15.5. SERVIÇO DE ANÁLISE DA QUALIDADE

**15.5.1.** Será executado por profissionais especializados e certificados na ferramenta Sistema de monitoração para cibersegurança e qualidade operacional;

**15.5.2.** Os dados de performance e capacidade a serem analisados deverão ser providos unicamente pelas ferramentas de Network Performance Management (NPM) e Application Performance Management (APM), utilizados pela Contratante. Não cabe a Contratada a instalação ou manutenção dessas ferramentas, apenas o consumo de dados;

**15.5.3.** O serviço será prestado por equipe em regime de teletrabalho, com acesso

remoto às ferramentas de monitoração;

**15.5.4.** Cabe ao Contratante assegurar o acesso remoto aos recursos de monitoração, via VPN ou outras tecnologias, para viabilizar o serviço de análise de performance;

**15.5.5.** O serviço será prestado em horário comercial, em dias úteis, conforme calendário local da Contratante;

**15.5.6.** Esse serviço prevê a execução de análise profissional quanto a performance e qualidade de serviço de aplicações Web, banco de dados e infraestrutura;

**15.5.7.** As análises de performance serão feitas de acordo com a prioridade definida pela Contratante;

**15.5.8.** A Contratada terá um prazo de 24 (vinte e quatro) horas corridas para iniciar o serviço de análise após a solicitação formal;

**15.5.9.** Após o início da análise, a Contratada deverá concluir as atividades num prazo máximo de 48 (quarenta e oito) horas corridas;

**15.5.10.** As análises serão realizadas na ordem em que foram solicitadas e, caso a Contratante indique mais de um item por vez, deverá indicar a ordem de prioridade;

**15.5.11.** As análises serão realizadas sequencialmente, respeitando os prazos previstos para início e fim das atividades;

**15.5.12.** Cabe à Contratante definir o escopo da análise, detalhando:

a) Endereços IP dos servidores onde estão os serviços que serão analisados;

b) Nome dos serviços e portas TCP/UDP;

c) Topologia de rede.

**15.5.13.** A análise deve incluir os seguintes aspectos:

a) Performance de resposta dos servidores de aplicação, banco de dados, webservices e outros componentes da aplicação;

b) Melhoria do tempo de resposta e experiência do usuário final;

c) Requisições com maiores tempos de resposta e sugestões de melhorias;

d) Requisições que apresentaram erros em execução e sugestões de melhorias;

e) Problemas relativos à gargalos em rede e interfaces de comunicação (ex. retransmissões e zero window);

f) Falhas em balanceamento de carga;

g) Falhas em DNS;

h) Erros de autenticação;

i) Lentidão no acesso a FTP ou sistemas NAS (Network AttachedStorage), SMB e NFS;

j) Possíveis razões de erros em HTTP, com análise do conteúdo das transações;

k) Queries lentas ou com erros em sistemas de banco de dados, com sugestões de melhorias;

l) Otimização de objetos estáticos (imagens, PDF, vídeos, textos), com melhores práticas de uso de cache e compressão;

m) Latência da comunicação em rede e Round Trip Time;

n) Erros e performance de comunicações criptografadas em SSL/TLS.

**15.5.14.** O resultado das análises será fornecido através de documentação formal e

personalizada, contendo todas os levantamentos executados, inclusive com gráficos e tabelas explanatórias e análises da causa-raiz dos problemas encontrados;

**15.5.15.** Toda a documentação produzida irá conter o contato (telefone e e-mail) do especialista responsável pela análise;

**15.5.16.** A Contratante poderá entrar em contato com os especialistas em horário comercial para sanar eventuais dúvidas;

**15.5.17.** A Contratada terá um prazo de 4 (quatro) horas úteis para responder às dúvidas colocadas e fazer possíveis ajustes na documentação produzida.

## 16. DOS RECURSOS ORÇAMENTÁRIOS

**16.1.** As despesas para atender à licitação estão programadas em dotação orçamentária própria, prevista no orçamento do Estado de Alagoas para o exercício de (20...), na classificação abaixo:

Gestão/Unidade:

Fonte:

Programa de Trabalho:

Elemento de Despesa:

PI:

**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**.

## 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____

_____

Assinatura

Documento assinado eletronicamente por **José Álvaro de Oliveira**, **Gerente** em 31/01/2022, às 13:21, 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