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 – SERVIÇOS CONTINUADOS SEM MDO COM DEDICAÇÃO EXCLUSIVA

PREGÃO ELETRÔNICO Nº (...)/(20...)

Processo Administrativo n° E:41506.0000000409/2022

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. Futura e eventual contratação, via sistema de registro de preços, de empresa especializada no fornecimento de solução, pelo menor valor global (lote único), de solução tecnológica baseada em softwares para inspeção e segurança de credenciais em rede e aplicações web contemplando serviços de suporte especializado, treinamento, manutenção preventiva e corretiva com atualização e upgrades de versões, conforme condições, quantidade e exigências a seguir estabelecidas:

Item	CATMAT/ CATSER	Descrição	Unidade de Medida	Quantidade
1	27499	Licença de uso para solução baseada em software para inspeção e segurança de credenciais em rede e aplicações WEB	USR	60000
2	26972	Serviço de Implantação e Configuração	UND	1
3	26972	Treinamento	UND	1

2.2. A contratação tem prazo de vigência até 12 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.

3. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. Conforme indicado no Planejamento Estratégico, estruturado para o período de 2019 a 2022, o ITEC desenvolve iniciativas e práticas com o objetivo de potencializar a governança da administração pública em Alagoas.

3.2. A presente Demanda será responsável por suportar o alcance de três dos principais objetivos estratégicos, no campo da tecnologia, quais sejam:

3.3. 1.3 – Fomentar o desenvolvimento de sistemas de forma integrada e padronizada.

3.4. 1.4 – Expandir a prestação de serviços.

3.5. 1.6 – Consolidar a centralização do Datacenter do governo do Estado de Alagoas no ITEC.

3.6. Importante destacar que os objetivos acima mencionados, possuem desdobramentos mais aprofundados e coadunam-se na busca de uma solução de tecnologia que possa prover e potencializar a Segurança e Inspeção de informações e dados Institucionais custodiados pelo ITEC, permitindo o desenvolvimento de mecanismos de proteção das informações reservadas e sigilosas, maior segurança na ampliação e na disponibilização dos dados abertos no sítio, portal e outras mídias do instituto, melhorias relacionadas aos processos de auditoria de dados, a intensificação do combate à corrupção, bem como a modernização da infraestrutura tecnológica, garantindo assim a sustentação e a modernização dos serviços de TI.

3.7. A justificativa para investir recursos na busca de uma Solução de Segurança e Inspeção de informações e dados institucionais, recai sobre a urgência na implementação de ferramentas e soluções que possam minimizar os pontos de falha de segurança dos sistemas em custódia, hospedados e processados no ITEC, garantindo assim a performance e disponibilidade das aplicações e sistemas, reduzindo a possibilidade de indisponibilidade de acesso aos serviços, bem como promovendo maior rastreabilidade quanto às tentativas de ataques efetuados dentro do ambiente computacional.

3.8. Nesse contexto, devido ao aumento significativo do número de ataques cibernéticos, potencializados pela “onda” crescente do uso de soluções de tecnologia e aplicações de TI, tem-se observado um significativo avanço do setor governamental, no sentido de direcionar esforços para a criação de diretrizes, atos normativos e legais, bem como o investimento de recursos relacionados ao tema Governança e Gestão de TI.

3.9. Espera-se que a solução a ser contratada seja capaz de gerar relatórios que suportem a efetividade dos controles de segurança, assim como, por meio de seus recursos e funcionalidades possibilite a auditoria de informações de acessos tanto de administradores quanto dos usuários, trazendo uma visão global e detalhada das permissões de acesso, modificações não necessárias aos recursos, arquivos ou caixas de correio, detectando atividades não autorizadas de processamento de informações, monitorando os eventos das caixas postais dos usuários e das pastas públicas, a análise comportamental dos usuários nos servidores.

3.10. A demanda encontra ainda o amparo da Visão do ITEC, na medida em que a solução que será futuramente contratada permitirá uma melhoria na Governança de informações de interesse do estado e do cidadão, propiciando a manutenção da imagem institucional do instituto, bem como a garantia da confiança da população e estado, sendo uma referência entre entidades estaduais de TIC.

3.11. Com base em todo o contexto, a demanda justifica-se em razão da necessidade de se desenvolver estratégias que possam inibir a tentativa de busca e vazamento de informações que possam comprometer a segurança de dados dos órgãos, cidadãos, secretarias e Autarquias no âmbito da administração pública hospedados no ITEC, bem como reduzir riscos de ataques ao ambiente computacional.

3.12. Importante ressaltar que as informações tratadas por essa Instituição são ativos valiosos para a eficiente prestação dos serviços públicos, é por este motivo que se busca, através da presente demanda, desenvolver ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, assegurando a qualidade dos serviços públicos esperados pela população, garantindo a segurança com relação à guarda de "dados sensíveis" pelo governo, através da adoção de medidas rigorosas de segurança para acesso dessas informações.

3.13. Por fim, busca-se estar em conformidade com as normas e padrões de segurança da informação trazidos pela Lei Geral de Proteção de Dados LGPD, aos preceitos legais que regem a responsabilidade sobre os dados gerados, armazenados, tratados e trafegados em ambiente desse Instituto.

3.14. Deste modo, resta justificada a necessidade do presente estudo, para avaliar as alternativas e requisitos para implantação de uma solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web contemplando serviços de suporte especializado, treinamento, manutenção preventiva e corretiva com atualização e upgrades de versões.

4. DOS REQUISITOS TÉCNICOS

A solução de inspeção e proteção de credenciais em aplicações de rede, web e mobile deverá atender, no mínimo, aos seguintes requisitos técnicos:

4.1. **Disponibilizar licenciamento com as seguintes capacidades mínimas de proteção e inspeção:**

4.1.1. Para inspeção e proteção de credenciais em aplicações web ou mobile: 60.000 (sessenta mil) credenciais;

4.1.2. Para inspeção e proteção de credenciais de alto privilegio no diretório de usuários internos: 100 (cem) credenciais;

4.1.3. Todas as licenças deverão ser fornecidas com suporte técnico, manutenção, garantia e atualização pelo período mínimo de 12 (doze) meses;

4.2. **Requisitos funcionais para inspeção e proteção de credenciais em aplicações web e mobile:**

4.2.1. Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação.

4.2.2. Assegurar a comunicação entre a solução e a aplicação web protegida através de criptografia de chaves simétricas.

4.2.3. Possibilitar a criação e configuração de politicas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política.

4.2.4. Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida.

4.2.5. Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida.

4.2.6. Possibilitar a definição de mais de uma fonte de autenticação para uma única aplicação web protegida.

4.2.7. Não exigir tokens, dispositivos móveis, códigos ou outras informações adicionais para o processamento de eventos.

4.2.8. Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos.

4.2.9. Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy.

4.2.10. Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.

4.2.11. Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet.

4.2.12. Identificar desvios no padrão de comportamento de uma credencial, possibilitando o envio de notificações, apresentação de desafios (token, captcha ou

similares) e bloqueio de acesso, a depender da política de risco definida.

4.2.13. Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança.

4.2.14. Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude.

4.2.15. Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e-mail, possibilitando a redação de mensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não.

4.2.16. Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificação recebida a veracidade do acesso.

4.2.17. Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida.

4.2.18. Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação.

4.2.19. Identificar ataques do tipo "força bruta", elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo.

4.2.20. A reputação das origens detectadas como geradores de ataques de força bruta devera? decair após determinado tempo, e o tempo de decaimento da reputação devera? aumentar em função da recorrência de tentativas de ataques de força bruta.

4.2.21. Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada em interface gráfica, com base na política de risco definida.

4.2.22. Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância.

4.2.23. Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando o nome do usuário (credencial) e score de risco acumulado.

4.2.24. Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento.

4.2.25. Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política.

4.2.26. Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento.

4.2.27. Possuir dashboard para visualização do risco organizacional em um intervalo

de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido.

4.2.28. Possuir integração com soluções do tipo "single-sign-on", disponibilizando no mínimo, de forma nativa, o RH-SSO.

4.2.29. Possuir integração nativa com a autenticação de tecnologias de mercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak.

4.2.30. Ser capaz de processar eventos originados em IPv4 e IPv6.

4.2.31. Possuir identificador único para todos os eventos processados pela solução.

4.2.32. Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis.

4.2.33. Disponibilizar console web responsiva para toda operação da solução.

4.3. **Requisitos funcionais para inspeção e proteção de credenciais de alto privilegio no diretório de usuários internos:**

4.3.1. A solução deverá ser compatível com Active Directory;

4.3.2. A solução deverá aprender o comportamento padrão dos usuários e dos recursos monitorados baseando-se nos eventos de auditoria coletados para identificar e alertar desvios e anormalidades nesses comportamentos;

4.3.3. A solução deverá ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;

4.3.4. A solução deverá permitir a configuração de alertas customizados para que um usuário, um período ou uma ação específica seja alertada caso ocorra ação que os envolva.

4.3.5. A solução deverá permitir a configuração de alertas em protocolos de integração com outras soluções como SNMP e Syslog.

4.3.6. A solução deverá permitir que os alertas sejam enviados por e-mail;

4.3.7. A solução deverá permitir que os alertas disparem a execução de respostas ou ações pré-configuradas ou através da execução de scripts.

4.3.8. A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalações de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de descoberta de contas com NTLM e Kerberos; Ataques de força bruta;

4.3.9. Os alertas deverão ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;

4.3.10. O dashboard deverá apresentar todos os eventos que motivaram o alerta para que o time de segurança possa fazer investigação forense;

4.3.11. A solução deverá exibir no dashboard todos os eventos ocorridos que

motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtradas, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.

4.3.12. O dashboard deverá possuir página com KPIs de compliance e segurança dos servidores e recursos monitorados e a partir desses KPIs, deve ser possível abrir a lista com informações detalhadas.

4.3.13. A solução deverá permitir integração com ferramentas de SIEM e outras soluções de gerenciamento de ativos.

4.4. **Requisitos funcionais do painel integrado de eventos inspeção e segurança de credenciais:**

4.4.1. Possuir mecanismo nativo para gestão de usuários que podem acessar o painel de visualização, incluindo minimamente integração nativa com os seguintes sistemas de diretório de usuários: Active Directory e Keycloak/RH-SSO.

4.4.2. Criptografar com chave simétrica toda a comunicação com as fontes geradoras de eventos.

4.4.3. Ao armazenar eventos em base de dados, anonimizar minimamente o campo que contem a informação de nome de usuário, seja este um CPF, matrícula, e-mail ou uma string qualquer (ex: nome.sobrenome).

4.4.4. As informações disponibilizadas no painel de visualização deverão estar sempre orientadas a um intervalo de datas.

4.4.5. Fornecer estatísticas dos eventos de segurança originados nas aplicações web, mobile e de rede protegidas pela solução.

4.4.6. Fornecer minimamente as seguintes estatísticas:

4.4.7. Usuários que mais geram eventos de segurança no ambiente Microsoft e nas aplicações web;

4.4.8. Endereços IPs que mais geram eventos de segurança no ambiente de rede e nas aplicações web;

4.4.9. Incidentes de segurança mais frequentes;

4.4.10. Permitir visualizar detalhes de cada evento de segurança coletado.

4.4.11. Permitir filtrar eventos por usuário (credencial);

4.4.12. Permitir filtrar eventos por endereço IP de origem;

5. DOS SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO

5.1. Por implantação e configuração entende-se a instalação das soluções que compõem o objeto no ambiente computacional do ITEC, bem como a ativação das respectivas licenças das ferramentas que compõem o referido objeto, pelo período de vigência e quantitativo requeridos no edital.

5.2. O serviço deverá ser executado mediante abertura de ordem de serviço, emitida em até 10 (dez) dias após a assinatura do contrato.

5.3. A CONTRATADA deverá apresentar Plano de Implantação e Configuração, detalhando requisitos, etapas, matriz de responsabilidade e prazos para execução das atividades.

5.4. O prazo para conclusão do processo de implantação e configuração da solução é de até 15 (quinze) dias úteis após a data de emissão da ordem de serviço.

5.5. Para fins de comprovação da execução do serviço de implantação e configuração, a contratada deverá elaborar e entregar relatório técnico com evidências do cumprimento do plano de implantação, bem como a comprovação da disponibilidade das licenças nos prazos e quantidades que serão especificados no edital e seus anexos.

6. DOS SERVIÇOS DE SUPORTE TÉCNICO, MANUTENÇÃO, GARANTIA E ATUALIZAÇÃO

6.1. Os serviços de suporte técnico aqui descritos serão prestados pelo período de 12 meses a partir da ativação das licenças.

6.2. A garantia dos produtos adquiridos, bem como o livre acesso a atualizações e patches, será de 12 (doze) meses, a partir da data do recebimento das licenças da solução.

6.3. A garantia contemplará atendimento técnico quanto à configuração e solução de problemas envolvendo o produto ofertado, bem como a atualização dos softwares.

6.4. O atendimento aos chamados de suporte técnico será prestado na modalidade remota.

6.5. Para solicitações de atendimento/abertura de chamados a CONTRATADA deverá dispor de portal web e linha telefônica local ou 0800.

6.6. Para os chamados de severidade 1 (um), o atendimento deverá ser em regime de disponibilidade 24x7x365.

6.7. Para os chamados de severidade 2 (dois), 3 (três) e 4 (quatro) o suporte deverá ser prestado das 8H as 18 h, de segunda-feira a sexta-feira, exceto feriados nacionais, conforme quadro a seguir:

Severidade	**Descrição**	**Tempo para início do Atendimento**
Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado	No máximo 2 (duas) horas após a abertura do chamado
Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	No máximo 4 (quatro) horas após a abertura do chamado
Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componentes	No máximo 12 (doze) horas após a abertura do chamado
		No máximo 24 (vinte e

Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto	(vinte e quatro) horas após a abertura do chamado

6.8. Os chamados de suporte deverão ser classificados de acordo com a sua criticidade e terão prazos de atendimento e solução especificados conforme acordo de nível de serviço definido neste termo de referência.

6.9. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento;

6.10. Mensalmente deverá ser entregue pela contratada um relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período com no mínimo as seguintes informações: número do contrato, período de referência, número de acionamento, localidade, severidade, descrição da ocorrência, nome do responsável pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, data e hora da solução e descrição da resolução adotada;

6.11. O não atendimento dos níveis de serviço preestabelecidos ensejarão a cobrança de multas conforme será indicado na minuta contratual.

7. DO TREINAMENTO

7.1. A Contratada deverá prestar serviços de treinamento aos funcionários indicados pelo ITEC, com as características descritas a seguir:

7.2. Uma turma para até 10 (dez), participantes com carga horária mínima de 08 (oito) horas;

7.3. As datas de aplicação dos treinamentos deverão ser fixadas de comum acordo com o ITEC;

7.4. O conteúdo do treinamento deverá abranger:

7.5. Apresentação da arquitetura da solução;

7.6. Visão geral de funcionamento de cada solução;

7.7. Todo o material didático deverá ser repassado de forma impressa e em mídia para os alunos;

7.8. O treinamento deverá ocorrer no formato remoto ou, a critério do ITEC, no formato presencial, ficando a mesma responsável por montar o ambiente adequado para realização do treinamento, isto é, todo o espaço necessário assim como toda infraestrutura computacional e de rede necessária;

7.9. Caberá à empresa contratada instalar a plataforma e demais softwares que compõem a solução ou possibilitar o acesso para o treinamento;

7.10. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da empresa contratada, incluindo os gastos com instrutores, alimentação, estadia e o seu deslocamento;

7.11. Para fins de comprovação da execução dos Serviços de Treinamento, a contratada deverá entregar:

7.12. Lista de presença dos participantes do treinamento;

7.13. Certificado de execução do treinamento para cada participante ao término do

treinamento.

7.14. O treinamento deverá ser executado em até 60 dias após o término do serviço de instalção e configuração.

8. DA MENSURAÇÃO DOS SERVIÇOS

Os serviços da futura contratação serão mensurados através dos seguintes critérios:

8.1. As licenças de software serão mensuradas em quantidade de usuários e pagas integralmente, em parcela única, por todo o período do contrato.

8.2. A Instalação e Configuração do software serão mensurados e pagos como atividade única, tendo sua verificação a partir da estabilização da Solução no ambiente do ITEC e da disponibilização das licenças.

8.3. O Treinamento será mensurado a partir de turmas, a serem demandadas por intermédio de agendamento a ser realizado de forma programada junto a empresa contratada, pagos após a realização dos serviços.

9. DO CRONOGRAMA DE EXECUÇÃO

A execução do projeto se dará conforme o cronograma abaixo indicado:

Descrição	Prazo
Ordem de Fornecimento	D
Entrega do projeto de implantação	D+5
Conclusão da Instalação e Configuração	D+15
Ativação e Disponibilização das Licenças e da Solução	D+15
Termo de Recebimento Provisório	D+20
Termo de Recebimento Definitivo Itens	D+30
Pagamento Itens 1 e 2	A partir do Termo Definitivo
Garantia e Suporte Técnico	A partir do Termo Definitivo
Treinamento	D+60

9.1. As licenças de software serão mensuradas e pagas integralmente, em parcela única, por todo o período do contrato.

9.2. A Instalação e Configuração do software serão mensurados e pagos como atividade única, tendo sua verificação a partir da estabilização da Solução no ambiente do ITEC e da disponibilização das licenças.

9.3. O Treinamento será mensurado a partir de turmas, a serem demandadas por intermédio de agendamento a ser realizado de forma programada junto a empresa contratada, pagos após a realização dos serviços.

10. DA PROPOSTA

10.1. Para suportar a análise técnica da oferta da empresa, na fase de Proposta, deverão ser apresentados catálogos técnicos/manuais/folder, bem como uma proposta técnica com a especificação clara e objetiva do objeto ofertado e roteiro de comprovação em planilha ponto-a-ponto, indicando documento e página que comprove cada requisito.

10.2. Haja vista a complexidade e alto impacto do projeto no ambiente computacional do ITEC, a empresa vencedora da etapa competitiva (após a fase de lances), será convocada a apresentar uma Prova de Conceito (POC) da solução ofertada conforme item específico neste TR, momento em que serão demonstrados os requisitos de maior relevância para uma correta análise e aferição da compatibilidade da solução com as especificações técnicas.

10.3. O roteiro de prova de conceito para viabiliza uma análise objetiva, por parte das empresas interessadas e pela área técnica da administração, está disponível no ANEXO II

TABELA 1

ITEM	DESCRIÇÃO	QTD	Unitário	R$
1	Licença de uso para solução baseada em software para inspeção e segurança de credenciais em rede e aplicações WEB	60000	R$	R$
2	Serviço de Implantação e Configuração	01	R$	R$
3	Treinamento	01	R$	R$
-	-	-	TOTAL	R$

11. DOS DOCUMENTOS DE HABILITAÇÃO

11.1. Para fins da análise de qualificação técnico operacional da empresa contratada deverão ser exigidos, com base no que dispõe a previsão legal, no mínimo 1 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando a experiência anterior da empresa no fornecimento/licenciamento de solução de segurança da informação, compatível e similar ao objeto licitado, compreendendo serviços de suporte técnico e instalação, atestando, inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais, no(s) atestado(s).

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

11.3. Características: execução de serviço continuado de compatibilidade com as características relevantes e significativas do objeto licitado;

11.3.1. Quantidades: no mínimo, 50% (cinquenta por cento) da quantidade do objeto licitado;

11.3.2. Prazos: no mínimo, 50% (cinquenta por cento) do prazo de execução do

objeto licitado.

12. DA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

12.1. O prazo de entrega dos bens é de 15 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, no endereço informado no ANEXO ÚNICO.

12.2. 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.

12.3. 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.

12.4. 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.

12.5. 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.

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

13. DA CLASSIFICAÇÃO DOS SERVIÇOS COMUNS

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

13.2. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

14. DOS REQUISITOS DA CONTRATAÇÃO

14.1. Conforme Estudos Preliminares, os requisitos da contratação abrangem o seguinte:

14.1.1. Considerando os objetivos esperados e a justificativa da demanda, a solução a ser contratada deverá prever no mínimo, as seguintes características, recursos e funcionalidades:

a) Solução baseada em software para inspeção e segurança de credenciais em rede e aplicações WEB;

b) Serviço de Implatação e Configuração;

c) Treinamento.

14.1.2. Dada a importância do objeto, em vistas ao atendimento da Lei Geral de Proteção de Dados, eventuais impactos operacionais e prejuízos oriundos de ameaças cibernéticas, os serviços são definidos de natureza continuada, e poderão

ser renovados por iguais e sucessivos períodos, desde que respeitados os limites legais, conforme determinação do art. 57 da lei 8666/93.

14.1.3. Quando restarem 03 (três) meses antes da data do efetivo término do contrato de prestação dos serviços de suporte e garantia, a CONTRATADA deverá realizar uma vistoria completa na solução e ambiente, de modo a prestar para o ITEC toda a assistência a fim de que os equipamentos continuem plenamente funcionais;

14.1.4. O fato de a CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pelo ITEC, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços, constituirá quebra de contrato, sujeitando-a às obrigações em relação a todos os danos causados ao ITEC pela falha;

14.1.5. A CONTRATADA compromete-se a fornecer para o ITEC toda a documentação relativa à prestação dos serviços de suporte e garantia que esteja em sua posse, tais como: arquitetura da solução, consumo do ambiente, incidentes em tratamento, e outras que venham a ser requeridas pelo Órgão durante a fase de transição.

14.2. Declaração de que tem pleno conhecimento das informações, condições e peculiaridades inerentes à natureza do serviço e ao local de sua execução, que assume total responsabilidade por esse fato e que não o utilizará para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a Contratante.

15. DA VISTORIA

15.1. Para o correto dimensionamento e elaboração de sua proposta, a licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhada por servidor designado para esse fim, de segunda a sexta-feira, das 8 horas às 12 horas e das 13 horas às 17 horas.

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

15.3. Para a vistoria, a licitante, ou o seu representante, deverá estar devidamente identificada, apresentando documento de identidade civil e documento expedido pela empresa, comprovando sua habilitação para a realização da vistoria.

15.4. Por ocasião da vistoria, à licitante, ou ao seu representante legal, poderá ser entregue CD-ROM, *pen-drive*, ou outra forma compatível de reprodução, contendo as informações relativas ao objeto da licitação, para que a empresa tenha condições de bem elaborar sua proposta.

15.5. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

16. DO MODELO DE EXECUÇÃO DO OBJETO

16.1. A execução do objeto seguirá a seguinte dinâmica:

16.1.1. O prazo de execução será contado, do efetivo recebimento da Ordem de Fornecimento/Execução, até a expiração do prazo de vigência contratual, observando cronograma físico-financeiro estabelecido neste termo de referência.

16.1.2. Os trabalhos deverçao ser executados remotamente ou nas dependências do ITEC, em horário comercial.

16.1.3. A CONTRATADA deverá 24x7 a disponibilidade e correto funcionamento das soluções fornecidas, emitindo relatório mensal com os índices aferidos, bem como lista dos registros de suporte técnico atendidos no período.

16.1.4. As licenças deverão ser acompanhadas de suporte técnico, garantia e direito a atualização de versão. Ao longo de todo o contrato o ITEC poderá a qualquer momento demandar apoio técnico através de chamados em plataforma disponibilizada pela CONTRATADA.

16.1.5. O ITEC deverá fornecer ambiente adequado para instalação das soluções, e acesso aos colaboradores da CONTRATADA quando necessário;

16.1.6. Não será admitida a participação de consórcio.

17. DOS MATERIAIS A SEREM DISPONIBILIZADOS

17.1. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades estabelecidas neste edital, promovendo sua substituição quando necessário.

17.1. Para a perfeita execução dos serviços, a Contratante irá disponibilizar em seu ambiente computacional os seguintes recursos:

17.1.1. Um servidor físico ou virtual, para executar a solução a ser contratada, com no mínimo 8 núcleos de CPU, 32GB de RAM e 500Gb de espaço para armazenamento. Sistema operacional Linux.

17.1.2. Um servidor físico ou virtual, para executar a solução a ser contratada, com no mínimo 8 núcleos de CPU, 32GB de RAM e 500Gb de espaço para armazenamento. Sistema operacional Windows Server.

18. DAS OBRIGAÇÕES DA CONTRATANTE

18.1. São obrigações da Contratante:

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

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

18.1.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

18.1.4. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

18.1.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da Contratada, no que couber.

18.1.6. Não praticar atos de ingerência na administração da Contratada, tais como:

18.1.6.1. Exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

18.1.6.2. Direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

18.1.6.3. Promover ou aceitar o desvio de funções dos trabalhadores da Contratada, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado; e

18.1.6.4. Considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens;

18.1.7. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

18.1.8. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

18.1.9. Cientificar o órgão de representação judicial da Procuradoria Geral do Estado para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

18.1.10. Arquivar, entre outros documentos, projetos, *as built*, especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas.

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

18.1.12. 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;

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

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

18.1.15. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos.

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

19. DAS OBRIGAÇÕES DA CONTRATADA

19.1. 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:

19.1.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito

cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

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

19.1.3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao Estado de Alagoas ou à entidade estadual, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

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

19.1.5. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a Contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, documentação mencionada nos arts. 28, 29 e 31 da Lei nº 8.666, de 1993.

19.1.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

19.1.7. 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 n° 8.078, de 1990);

19.1.8. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;

19.1.9. Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução dos serviços;

19.1.10. Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

19.1.11. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato;

19.1.12. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado;

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

19.1.14. Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo;

19.1.15. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos,

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

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

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

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

19.1.19. 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);

19.1.20. 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;

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

19.1.22. 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;

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

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

19.1.24. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a Contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015;

19.1.25. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

19.1.26. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993;

19.1.27. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

19.1.28. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

19.1.29. Assegurar à Contratante:

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

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

19.1.30. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, exigida, inclusive, a capacitação dos técnicos da Contratante ou da nova empresa que continuará a execução dos serviços, sempre que necessário.

20. DA SUBCONTRATAÇÃO

20.1. Não será admitida a subcontratação do objeto licitatório.

21. ALTERAÇÃO SUBJETIVA

21.1. É admissível a fusão, cisão ou incorporação da Contratada com ou 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.

22. DO GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS

22.1. 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:

22.1.1. Providenciar a assinatura da Ata de Registro de Preços e o encaminhamento de sua cópia aos órgãos ou entidades participantes;

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

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

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

22.1.5. 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;

22.1.6. Formalizar o cancelamento do registro do fornecedor.

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

23. DO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

23.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993.

23.1.1. Fica-se indicado como fiscal de contrato os servidores: Juliano Araújo Farias, Gerente de Operações, matrícula 54254-7, juliano.araujo@itec.al.gov.br; Fabrício Dias Bittencourt, Gerente Executivo Administrativo, matrícula 9865922-7, fabricio.dias@itec.al.gov.br; Joel Salgueiro Bem Neto, Assessor Técnico de Contratos e Convênios, matrícula 57-4, joel.salgueiro@itec.al.gov.br.

23.2. O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

23.3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

23.4. A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

23.5. A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

23.6. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

23.7. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 87 da Lei nº 8.666, de 1993.

23.8. As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

23.9. A fiscalização técnica dos contratos avaliará constantemente a execução do objeto e, em sendo o caso, utilizará o Instrumento de Medição de Resultado (IMR), conforme modelo anexo, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a Contratada:

23.9.1. Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

23.9.2. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

23.10. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

23.11. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à Contratada a correção das faltas, falhas e irregularidades constatadas.

23.12. O fiscal técnico deverá apresentar ao preposto da Contratada a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

23.13. Em hipótese alguma, será admitido que a própria Contratada materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

23.14. A Contratada poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador;

23.15. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à Contratada de acordo com as regras previstas no ato convocatório.

23.16.O fiscal técnico poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

23.17. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha sua relação detalhada, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

23.18. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

23.18.1. Reuniões mensais entre a equipe de gestão do contrato e a CONTRATADA com o seguinte escopo

a) Avaliação da qualidade do serviço prestado, considerando relatórios mensais e observância dos prazos de atendimento;

b) Manutenção do pleno atendimento da solução e da contratada aos requisitos estabelecidos no termo de referência.

23.19. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

24. DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

24.1. A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

24.2. No prazo de até 5 dias corridos, do adimplemento da parcela, a Contratada deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual.

24.3. O recebimento provisório será realizado pelo fiscal técnico e setorial ou pela equipe de fiscalização após a entrega da documentação acima, da seguinte forma:

24.3.1. A Contratante realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários;

24.3.2. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à Contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

24.3.3. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

24.3.4. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis;

24.3.5. No prazo de até 10 dias corridos, a partir do recebimento dos documentos da Contratada, cada fiscal ou a equipe de fiscalização deverá elaborar relatório circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato;

24.3.6. Quando a fiscalização for exercida por um único servidor, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo;

24.3.7. Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último;

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

24.4. No prazo de até 10 (dez) dias corridos, a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o atesto da execução dos serviços, obedecendo as seguintes diretrizes:

24.4.1. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

24.4.2. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

24.4.3. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização, com base, se for o caso, no Instrumento de Medição de Resultado (IMR).

24.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei n° 10.406, de 2002).

24.6. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos, refeitos ou substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de sanções.

25. DO PAGAMENTO

25.1. 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.

25.1.1. 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.

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

25.3. A emissão da Nota Fiscal ou Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência.

25.4. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da manutenção das condições de habilitação exigidas no edital, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada nos arts. 28, 29 e 31 da Lei nº 8.666, de 1993.

25.5. O setor competente para proceder ao pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

25.5.1. O prazo de validade;

25.5.2. A data da emissão;

25.5.3. Os dados do contrato e da Contratante;

25.5.4. O período de prestação dos serviços;

25.5.5. O valor a pagar; e

25.5.6. Eventual destaque do valor de retenções tributárias cabíveis.

25.6. 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.

25.7. Tendo sido definidos parâmetros para mensuração do percentual do pagamento devido em razão dos níveis esperados de qualidade da prestação do serviço, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

25.7.1. Não produziu os resultados acordados;

25.7.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

25.7.3. Deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

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

25.9. 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.

25.9.1. 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.

25.10. 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.

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

25.11. 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.

25.12. 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.

25.13. 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.

25.13.1. 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.

25.14. 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.

25.15. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no art. 31 da Lei 8.212, de 1993, quando couber.

25.16. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar n° 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.

26. DO REAJUSTE

26.1. Os preços são fixos e irreajustáveis no prazo de um ano, contado da data limite para a apresentação das propostas.

26.2. Na hipótese de prorrogação extraordinária, na forma do art. 57, §1°, da Lei n° 8.666, de 1993, fica assegurada a manutenção de seu equilíbrio econômico-financeiro, aplicando-se o índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, contada da data limite para a apresentação das propostas.

27. DA GARANTIA DE EXECUÇÃO

27.1. O adjudicatário, no prazo de 10 (dez) dias úteis após a assinatura do Termo de Contrato ou o aceite do instrumento equivalente, prestará garantia no valor correspondente a 5% do valor do contrato, a qual será liberada conforme o disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.

27.1.1. A inobservância do prazo fixado para a prestação da garantia autoriza a Contratante a promover o bloqueio dos pagamentos devidos à Contratada, até o limite de 5% do valor do contrato, a título de garantia, ou a rescindir o contrato, nos termos da Lei nº 8.666, de 1993.

27.1.2. O bloqueio efetuado não gera direito a nenhum tipo de compensação financeira à Contratada.

27.1.3. A Contratada, a qualquer tempo, poderá substituir o bloqueio efetuado por quaisquer das modalidades de garantia.

27.2. Caberá à Contratada optar por uma das seguintes modalidades de garantia:

27.2.1. Caução em dinheiro ou em títulos da dívida pública, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

27.2.2. Seguro-garantia;

27.2.3. Fiança bancária.

27.3. A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal, em conta específica, com correção monetária, em favor da Contratante.

27.4. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

27.5. Se o valor da garantia for utilizado total ou parcialmente em pagamento de

qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 10 dias úteis, contados da data em que for notificada.

27.6. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

27.7. A garantia prestada pela Contratada será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente.

28. DAS SANÇÕES ADMINISTRATIVAS

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

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

28.1.2. Não entregar a documentação exigida no edital;

28.1.3. Apresentar documentação falsa;

28.1.4. Causar o atraso na execução do objeto;

28.1.5. Não mantiver a proposta;

28.1.6. Falhar na execução do contrato;

28.1.7. Fraudar a execução do contrato;

28.1.8. Comportar-se de modo inidôneo;

28.1.9. Declarar informações falsas; e

28.1.10. Cometer fraude fiscal.

28.2. As sanções do subitem 31.1. 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.

28.3. 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:

28.3.1. 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

28.3.2. Multa.

28.4. 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.

28.5. 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.

28.5.1. 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.

28.6. 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.

28.7. 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.

28.8. 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.

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

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 serviços 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.

Município de Maceió, 14 de novembro de 2022.

ANEXO I
MODELO DE PROPOSTA DE PREÇO

(papel timbrado)

À

Agência de Modernização da Gestão de Processos – AMGESP

Ref.: Pregão Eletrônico SRP No XX

Processo Administrativo n° E:41506.0000000409/2022

Prezados Senhores,

Após examinar todas as especificações e condições constantes do TERMO DE REFERÊNCIA, apresentamos nossa proposta comercial para fornecimento de solução tecnológica baseada em softwares para inspeção e segurança de credenciais em

rede e aplicações web contemplando serviços de suporte especializado, treinamento, manutenção preventiva e corretiva com atualização e upgrades de versões, pelo período de 12 meses, para atender as necessidades do ITEC-AL.

PLANILHA DE PROPOSTA DE PREÇOS

ITEM	DESCRIÇÃO	QTD	Valor Unitário	Valor Total
1	Licença de uso para solução baseada em software para inspeção e segurança de credenciais	60.000	R$	R$
2	Serviço de Implantação e Configuração	01	R$	R$
3	Treinamento	01	R$	R$
-	-	-	TOTAL	R$

1) Dados da Proposta:

Valor Total R$_____ (valor por extenso).

2) Validade da Proposta: 60 (sessenta) dias

3) Informamos, por oportuno, que nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

4) Dados da empresa:

Razão Social: _____

CNPJ (MF) nº _____

Inscrição Estadual nº: _____

Endereço: _____

Telefone: _____ Fax: _____ e-mail: _____

Cidade: _____ Estado: _____

CEP: _____

5) Representante(s) legal(is) com poderes para assinar o contrato:

Nome: _____

Cargo: _____

CPF: _____ RG: _____ _____-____

6) Dados Bancários:

Banco:_____

Agência:_____

Conta Corrente:_____

7) Dados para Contato:

Nome: _____

Telefone/Ramal: _____

Declaramos que estamos em Situação Regular perante a Fazenda Estadual, a Seguridade Social e Fundo de Garantia por Tempo de Serviço, atendendo também as exigências do presente Edital quanto à habilitação jurídica e qualificações técnica e econômico-financeira, bem como que não possuímos, no nosso quadro funcional, menores de dezoito anos, em trabalho noturno, perigoso ou insalubre, e nem menores de dezesseis anos em qualquer atividade, salvo como aprendiz, nos termos da Lei n.º 9.854/99, regulamentada pelo Decreto n.º 4.358, de 05/09/2002.

Caso nos seja adjudicado o objeto do Contrato, informamos que o Sr. _____ (nome completo), portador do CPF/MF n.º _____ e, da C.I. n.º _____, residente e domiciliado(a) na _____, n.º _____, bairro _____, CEP.: _____, é o(a) nosso(a) representante e está devidamente autorizado(a) e credenciado(a) a receber quaisquer comunicações relacionadas com o Instrumento Contratual, cujo pagamento deverá ser depositado no Banco _____, Agência _____, na Conta Corrente _____.

Atenciosamente,

PROPONENTE _____

Por _____

Cargo _____

Fone/Fax_____

E-mail_____

ANEXO II

ROTEIRO DE PROVA DE CONCEITO

ITEM	DESCRIÇÃO	ATENDE	NÃO ATENDE
	Funcionalidades de inspeção e segurança de credenciais em aplicações web e mobile		
1	Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o		

1	nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação.		
2	Assegurar a comunicação entre a solução e a aplicação web protegida através de criptografia de chaves simétricas.		
3	Possibilitar a criação e configuração de politicas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política.		
4	Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida.		
5	Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida.		
6	Possibilitar a definição de mais de uma fonte de autenticação para uma única aplicação web protegida.		
7	Não exigir tokens, dispositivos móveis, códigos ou outras informações adicionais para o processamento de eventos.		
8	Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos.		
9	Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy.		
10	Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.		
11	Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet.		

12	Identificar desvios no padrão de comportamento de uma credencial, possibilitando o envio de notificações, apresentação de desafios (token, captcha ou similares) e bloqueio de acesso, a depender da política de risco definida.		
13	Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança.		
14	Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude.		
15	Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e-mail, possibilitando a redação de mensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não.		
16	Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificação recebida a veracidade do acesso.		
17	Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida.		
18	Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação.		
19	Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo.		
20	A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta.		
21	Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada		

21	em interface gráfica, com base na política de risco definida.		
22	Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância.		
23	Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando o nome do usuário (credencial) e score de risco acumulado.		
24	Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento.		
25	Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política.		
26	Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento.		
27	Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido.		
28	Possuir integração com soluções do tipo “single-sign-on”, disponibilizando no mínimo, de forma nativa, o RH-SSO.		
29	Possuir integração nativa com a autenticação de tecnologias de mercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak.		
30	Ser capaz de processar eventos originados em IPv4 e IPv6.		
31	Possuir identificador único para todos os eventos		

31	processados pela solução.		
32	Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis.		
33	Disponibilizar console web responsiva para toda operação da solução.		
	Funcionalidades de inspeção e segurança de credenciais em ambiente de rede:		
34	A solução deverá ser compatível com Active Directory;		
35	A solução deverá aprender o comportamento padrão dos usuários e dos recursos monitorados baseando-se nos eventos de auditoria coletados para identificar e alertar desvios e anormalidades nesses comportamentos;		
36	A solução deverá ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;		
37	A solução deverá permitir a configuração de alertas customizados para que um usuário, uma pasta, um período ou uma ação específica seja alertada caso ocorra ação que os envolva.		
38	A solução deverá permitir a configuração de alertas em protocolos de integração com outras soluções como SNMP e Syslog.		
39	A solução deverá permitir que os alertas sejam enviados por email;		
40	A solução deverá permitir que os alertas disparem a execução de respostas ou ações pré-configuradas ou através da execução de scripts.		
41	A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalações de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em		

	dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de decoberta de contas com NTLM e Kerkeros; Ataques de força bruta;		
42	Os alertas deverão ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;		
43	O dashboard deverá apresentar todos os eventos que motivaram o alerta para que o time de segurança possa fazer investigação forense;		
44	A solução deverá exibir no dashboard todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtradas, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.		
45	O dashboard deverá possuir página com KPIs de compliance e segurança dos servidores e recursos monitorados e a partir desses KPIs, deve ser possível abrir a lista com informações detalhadas.		
46	A solução deverá permitir integração com ferramentas de SIEM e outras soluções de gerenciamento de ativos.		
	Funcionalidades do painel integrado de eventos de inspeção e segurança de credenciais		
47	Disponibilizar console web responsiva para toda operação da solução.		
48	Possuir mecanismo nativo para gestão de usuários que podem acessar o painel de visualização, incluindo minimamente integração nativa com os seguintes sistemas de diretório de usuários: Active Directory e Keycloak/RH-SSO.		
49	Criptografar com chave simétrica toda a comunicação com as fontes geradoras de eventos.		
	Ao armazenar eventos em base de dados,		

50	anonimizar minimamente o campo que contem a informação de nome de usuário, seja este um CPF, matrícula, e-mail ou uma string qualquer (ex: nome.sobrenome).		
51	As informações disponibilizadas no painel de visualização deverão estar sempre orientadas a um intervalo de datas.		
52	Fornecer estatísticas dos eventos de segurança originados nas aplicações web, mobile e de rede protegidas pela solução		
53	Fornecer minimamente as seguintes estatísticas:		
54	a) Usuários que mais geram eventos de segurança no ambiente Microsoft e nas aplicações web;		
55	b) Endereços IPs que mais geram eventos de segurança no ambiente Microsoft e nas aplicações web;		
56	c) Incidentes de segurança mais frequentes;		
57	Permitir visualizar detalhes de cada evento de segurança coletado.		
58	Permitir filtrar eventos por usuário (credencial);		
59	Permitir filtrar eventos por endereço IP de origem.		

TR - Pregão - Serviços Continuados Sem MDO Exclusiva

Documento assinado eletronicamente por **Juliano Araújo Farias**, **Gerente** em 16/11/2022, às 10:03, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Joel Salgueiro Bem Neto**, **Assessor Técnico** em 16/11/2022, às 10:35, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **FABRICIO BITTENCOURT DIAS**, **Gerente** em 16/11/2022, às 10:50, 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 **15477347** e o código CRC **46EA7721**.