1. OBJETO

Trata-se de Registro de Preço para contratação de empresa especializada para o fornecimento de plataforma em nuvem para detecção e remediação de ataques digitais avançados por meio de inteligência artificial e análise comportamental para proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento, a fim de atender a demanda da Divisão de Suporte a Serviços de TI, subordinada à Diretoria de Tecnologia da Informação da Presidência do Tribunal de Justiça do Estado de Goiás.

Lote	Item	Descrição do Item	Métrica	Quantidade
1	1	Subscrição (assinatura de uso) anual da plataforma em nuvem para detecção e remediação de ataques digitais avançados por meio de inteligência artificial e análise comportamental para proteção de dispositivos.	Unidade de dispositivo	20.000
	2	Serviço de suporte técnico com operação assistida e transferência de conhecimento	Mês	12

Tabela 01 – Descrição resumida do objeto

2. JUSTIFICATIVA

O Tribunal de Justiça do Estado de Goiás (TJGO) vem investindo continuamente em Segurança da Informação e possui atualmente, dentre as suas soluções de segurança, soluções de antimalware (antivírus) para proteção de suas estações de trabalho e computadores servidores. Entretanto, com a evolução da tecnologia e sofisticação dos ataques, as ameaças não se restringem mais a artefatos maliciosos. Os ataques direcionados e coordenados, muitas vezes com a utilização de ferramentas do próprio sistema operacional têm sido cada vez mais comuns e vêm causando prejuízos a grandes organizações ao redor do mundo.

O processo de detecção e resposta a este tipo de ameaça necessita de plataformas e tecnologias mais avançadas de processos e operações (baseadas em análise comportamental e inteligência artificial) que, muitas vezes, não são percebidas pelas soluções tradicionais (baseadas em assinaturas de vírus/ataques). A capacidade de rastrear os eventos significativos de uma ocorrência, investigar o ataque correlacionando-o com o framework MITRE ATT&CK™ (https://attack.mitre.org/) e de responder ao ataque para impedir a sua continuação, eliminando os pontos de comprometimento, são fundamentais para uma estratégia de segurança bem-sucedida.

Em um cenário de mudanças constantes, exige-se a utilização de plataformas integradas e que se adaptem as exigências destes novos desafios frente a ataques digitais avançados. O aparato tecnológico em questão necessita demonstrar uma maior assertividade, devendo ser altamente capaz de detectar condutas desviantes no ambiente computacional, fornecendo uma capacidade de mitigação imediata para investigação, identificação e erradicação de ameaças, mantendo atualizações constantes no intuito de proteger o ambiente de novos ataques em potencial.

Nesse sentido, durante a fase de Estudo Técnico Preliminar (ETP), a equipe técnica de suporte ao planejamento dessa contratação realizou diversos estudos e análises, inclusive, por meio de Provas de Conceito (POC), identificou a alternativa tecnológica que melhor adaptou à sua realidade tecnológica. Como resultado desse trabalho, plataformas de segurança cibernética que fazem uso de inteligência artificial e análise comportamental mostraram um maior desempenho de segurança no ambiente tecnológico do TJGO, sendo, por consequência, objeto da presente contratação.

Importante ressaltar que, de acordo com a Resolução nº 370/2021, do Conselho Nacional de Justiça, em sua Seção II, Artigo 35, *"Recomenda-se utilizar serviços em nuvem que simplificam a estrutura física, viabilizam a integração, requisitos aceitáveis de segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário"* sendo, portanto, de suma importância iniciar a migração dos serviços essenciais de tecnologia em uso no TJGO para um ambiente em nuvem.

Dessa forma, por se tratar de tecnologia imprescindível para a segurança da informação do TJGO, mostra-se vital a contratação de tal plataforma/solução tecnológica no ambiente em nuvem para detecção e remediação de ataques digitais avançados por meio de inteligência artificial e análise comportamental, visto que a falta da contratação acarretará sérios riscos frente a ataques digitais avançados para o TJGO, especialmente no que tange a informações sensíveis e confidenciais.

Esta contratação aumentará significativamente a prevenção contra ataques avançados como ransomware e outros, além de tentativas de invasão aos sistemas de informação do TJGO, evitando problemas que possam prejudicar a disponibilidade e integridade dos serviços prestados a sociedade, garantindo o desempenho estável das estações de trabalho e computadores servidores de rede, disponibilizando melhores condições e nível de proteção aos usuários na realização de suas atividades administrativas e judiciais.

Assim, constitui objeto deste projeto a contratação de empresa especializada para o fornecimento de plataforma em nuvem para detecção e remediação de ataques digitais avançados por meio de inteligência artificial e análise comportamental para proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento, a fim de atender a demanda da Divisão de Suporte a Serviços de TI, subordinada à Diretoria de Tecnologia da Informação da Presidência do Tribunal de Justiça do Estado de Goiás.

Por fim, a presente contratação encontra-se alinhada com o Plano de Gestão do Poder Judiciário do Estado de Goiás para o biênio 2023-2025:

- Meta 04: Atingir o percentual de 50% no índice de desempenho de sustentabilidade até atingir o final do biênio;
- Meta 06: Atingir o percentual de 90% - nível de excelência no IGOVTIC-JUD;
- Meta 07: Alcançar no mínimo 75% no Prêmio CNJ de Qualidade.

Alinhada também com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026:

- Objetivo 01: aumentar a satisfação dos usuários do sistema judiciário;
- Objetivo 02: promover a transformação digital;
- Objetivo 05: aperfeiçoar a governança e a gestão;
- Objetivo 07: aprimorar a segurança da informação e a gestão de dados;
- Objetivo 08: promover serviços de infraestrutura e soluções corporativas.

3. BENEFÍCIOS E OBJETIVOS DA CONTRATAÇÃO

São benefícios e objetivos da contratação, entre outros:

a) Manter, neste Tribunal, os serviços de TI com excelência, com ferramentas e recursos avançados, permitindo projetar uma redução do tempo de resposta às demandas operacionais internas;
b) Aumentar a segurança e proteção dos dispositivos que compõem o parque computacional e o ambiente de rede do TJGO, fornecendo à equipe de TI alertas

para tomada de ações quanto a correção de infecções digitais que estejam sendo exploradas por atores maliciosos;

c) Dispor de painel gráfico em nuvem em tempo real para acesso via browser possibilitando analisar informações das atividades de proteção e possíveis ataques explorando vulnerabilidades existentes nos dispositivos do ambiente computacional do TJGO;
d) Melhorar o controle e a prevenção de ameaças que utilizam amplo espectro de técnicas de coleta de inteligência, não se restringindo a um único arquivo binário malicioso em qualquer dispositivo do TJGO;
e) Aumentar a prevenção e a remediação em relação a ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia, e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais em todos os dispositivos do TJGO protegidos pela solução;
f) Possibilitar o aumento da mitigação de riscos de ameaças em todo ambiente computacional do TJGO e seus dispositivos, que utilizam falhas recentes e não divulgadas dos sistemas operacionais (zero day exploits);
g) Proporcionar em todos os dispositivos do ambiente do TJGO, a prevenção e remediação de tipos de ameaças que usam técnicas de dividir o ataque em diversas fases podendo, por exemplo, controlar um grande número de equipamentos para diferentes finalidades, de modo que diferentes partes da infraestrutura-alvo sejam utilizadas em cada uma das fases do possível ataque;
h) Reduzir o risco de ameaças que utilizam técnicas de persistência com o direcionamento do ataque conduzido por uma interação e um monitoramento contínuo, até que se alcance um objetivo de invasão e ataque, não buscando apenas oportunidades eventuais nos dispositivos do TJGO;
i) Evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers, reduzindo o risco dos dispositivos, serviços e sistemas tecnológicos do TJGO serem acessados sem autorização;
j) Proporcionar consultas para auditoria por meio de Dashboard das detecções mais recentes, a quantidade de novas detecções e as que aconteceram por táticas nos últimos 30 dias, sendo possível reportar de forma agrupada para os dispositivos do ambiente de rede do TJGO;
k) Prover a melhoria e automação dos fluxos de trabalho, onde estejam sendo realizados manualmente pelas equipes de TI do TJGO, reduzindo os prazos de execução e custos operacionais;
l) Economia de recursos pela simplificação dos processos, redução no consumo de recursos humanos e melhoria nos fluxos de trabalho.
m) Melhorar o controle, gerência e manutenção dos recursos e funcionalidades disponibilizados pela DTI (Diretoria de Tecnologia da Informação) aos usuários do TJGO;
n) Otimização dos recursos de TI;
o) Melhorar critérios de segurança e governabilidade;
p) Aderência aos padrões e melhores práticas de mercado;
q) Melhorar o desempenho e disponibilidade dos serviços do TJGO;
r) Continuidade do negócio;
s) Satisfação dos usuários.

4. DO PARCELAMENTO DO OBJETO (DIVISÃO EM LOTES/ITENS)

Trata-se de contratação de solução de segurança tecnológica, em que os itens que a compõe, estão discriminados individualmente (Itens 1 e 2). Logo, a concorrência (julgamento das propostas) será realizada no formato MENOR PREÇO POR LOTE.

Não é possível falar em concorrência individualizada/separada entre os itens que compõem a solução tecnológica, uma vez que o serviço de suporte técnico com operação assistida e transferência de conhecimento (Item 2), está vinculado à plataforma/solução tecnológica a ser entregue no Item 1, sendo, portanto, interdependentes.

Dessa forma, as propostas comerciais deverão apresentar o valor de cada item, sendo que o preço global proposto deverá atender à totalidade da quantidade exigida, não sendo aceitas aquelas que contemplem apenas parte do objeto.

Nesse contexto, o parcelamento buscou cumprir o que está previsto nos arts. 15, IV e 23, §1º da Lei n° 8.666/93:

> Art. 15. As compras, sempre que possível, deverão: (…)
> IV - ser subdivididas em tantas parcelas quantas necessárias para aproveitar as peculiaridades do mercado, visando economicidade;
> Art. 23 (…) § 1o As obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

Por fim, essa separação por Lote/Itens dá transparência aos valores individuais e aumenta a participação das empresas no certame, além de propiciar a obtenção da proposta mais vantajosa para a Administração.

5. CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO

As especificações técnicas, características e observações acerca do objeto de contratação estão detalhadas no Anexo I deste Termo de Referência.

Outros requisitos gerais (comuns a todos os itens):

- Todos os requisitos dos itens contratados devem ser entregues licenciados. Palavras como: deve, permite, suporta, efetua, proporciona, possui e etc, significam que a funcionalidade deve ser entregue operacional, sem ônus adicional ao Tribunal.
- Caso o objeto seja de origem importada, a empresa licitante deverá, no momento da entrega do objeto, declarar se o adquiriu no mercado interno ou, diretamente, no mercado externo, quando deverá comprovar plena quitação dos tributos de importação a ele referentes, sob pena de rescisão contratual e multa, conforme prescreve o Inc. III, Art. 3º, do Decreto 7.174/2010.

6. CLASSIFICAÇÃO DOS BENS E SERVIÇOS

Os bens e serviços que constituem o objeto desta contratação são caracterizados como bens/serviços comuns, em conformidade à Lei nº 10.520/2002 e ao Decreto nº 7.174/2010, por possuir especificações usuais de mercado, nos termos dos referidos diplomas legais.

Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

7. DA VIGÊNCIA, LOCAL E PRAZO DE ENTREGA, GESTÃO E FISCALIZAÇÃO DO CONTRATO

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

O período de vigência do contrato objeto deste Termo de Referência será de **12 (doze) meses** a partir da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos mediante termos aditivos, até o limite de 48 (quarenta e oito) meses, após a verificação da real necessidade e das vantagens para a Administração quanto à continuidade do Contrato, para cada exercício financeiro, nos termos do artigo 57, II da Lei nº 8.666/93.

A possibilidade de renovação contratual se aplica ao Item 1 (Subscrição/assinatura de uso da solução tecnológica), bem como ao Item 2 (Serviço de suporte técnico com operação assistida e transferência de conhecimento), que compõem o objeto deste Termo de Referência.

Caso as partes não se interessem pela prorrogação deste contrato, deverão manifestar sua vontade, no mínimo, **120 (cento e vinte) dias** antes do término da vigência contratual.

No ato da entrega, o TJGO fará o recebimento provisório, para efeito de posterior verificação de conformidade com a especificação definida neste Termo de Referência. Uma vez assinado o contrato, os serviços deverão ser prestados conforme a tabela a seguir:

Item	Prazo Máximo para a Contratada entregar o objeto	Prazo Máximo para o TJGO emitir o Termo de Recebimento Definitivo	Responsável pelo recebimento provisório	Responsável pelo recebimento definitivo
1	A CONTRATADA tem o prazo de 45 (quarenta e cinco) dias corridos, após a assinatura do contrato, para entregar o objeto. Dentro desse prazo está contemplada a entrega das subscrições, bem como sua implantação no parque computacional do TJGO O ITEM 1 só será aceito definitivamente mediante a conclusão da etapa de Implantação.	5 (cinco) dias úteis após a entrega do objeto	Divisão de Suporte a Serviços de TI, subordinada à Diretoria de Tecnologia da Informação da Presidência	Divisão de Suporte a Serviços de TI, subordinada à Diretoria de Tecnologia da Informação da Presidência
2	O Item 2 será iniciado imediatamente mediante a conclusão da implantação e aceite do TJGO em relação ao Item 1.	5 (cinco) dias úteis após o encerramento de cada mês de prestação do serviço	Divisão de Suporte a Serviços de TI, subordinada à Diretoria de Tecnologia da Informação da Presidência	Divisão de Suporte a Serviços de TI, subordinada à Diretoria de Tecnologia da Informação da Presidência

Local de Entrega: Divisão de Suporte a Serviços de TI Palácio da Justiça – Av. Assis Chateaubriand, nº 195, Setor Oeste, CEP 74.130-011, Goiânia-GO Telefone: (62) 3216-4199, 3216-1190, 3216-8852 e 3216-1186 Contato: Valdemar Ribeiro, Marcus Vinícius ou Priscilla

Tabela 02 – Prazo máximo e local de entrega do objeto

7.1. CRONOGRAMA FÍSICO-FINANCEIRO

Segue o cronograma físico-financeiro do projeto:

Evento	Etapas	Prazo de Entrega	Responsável
1	Assinatura do contrato	Início (dia "D")	TJGO e CONTRATADA
2	Reunião inicial de alinhamento e assinatura do Termo de Compromisso e Sigilo de Informações	Em até 3 (três) dias uteis após a assinatura do contrato	TJGO e CONTRATADA
3	Elaboração do Plano de Implantação	Em até 8 (oito) dias uteis após a assinatura do contrato	CONTRATADA
4	Aprovação do Plano de Implantação	Em até 2 (dois) dias úteis após a entrega do "Evento 3"	TJGO
5	Execução do ITEM 1 deste Termo de Referência (Entrega das subscrições, instalação e configuração da solução/plataforma tecnológica)	Em até 45 (quarenta e cinco) dias corridos após a assinatura do contrato	CONTRATADA
6	Emissão do Termo de Recebimento Definitivo (ateste técnico) em relação ao ITEM 1 deste Termo de Referência, bem como, abertura interna do processo administrativo de pagamento em relação ao ITEM 1	Em até 5 (cinco) dias úteis após a entrega do "Evento 5"	TJGO
7	Início da prestação dos serviços contemplados no ITEM 2 deste Termo de Referência (Serviço de suporte técnico com operação assistida e transferência de conhecimento) Observação: O pagamento do ITEM 2 será iniciado a partir desta data. O pagamento do primeiro mês de serviço de suporte prestado, bem como, do último mês do ciclo do contrato, ocorrerá no formato pro rata die. Os demais meses serão pagos considerando o mês fechado (dia 1º ao 30º).	Início imediato	CONTRATADA
8	Emissão do Termo de Recebimento Definitivo (ateste técnico) em relação ao ITEM 2 deste Termo de Referência, bem como, abertura interna do processo administrativo de pagamento em relação ao ITEM 2	Em até 5 (cinco) dias úteis após o encerramento de cada mês de prestação do serviço	TJGO

Tabela 03 – Cronograma físico-financeiro

A execução do contrato será objeto de acompanhamento, controle, fiscalização e gestão dos seguintes integrantes:

Função	Nome	Cargo	Lotação	Matrícula
Gestor do Contrato	Valdemar Ribeiro da Silva Junior	Diretor de Divisão	DSSTI – DTI	5087210
Fiscal Administrativo	Marcus Vinícius Gonzaga Ferreira	Auxiliar Judiciário	DSSTI – DTI	5118190
Fiscal Técnico	Gabriel da Costa Ferro	Diretor de Serviço	DSSTI – DTI	5200131
Fiscal Técnico	Priscilla Elizabeth Pereira Batista	Analista Judiciário	DSSTI – DTI	5210403

Legenda: DSSTI – Divisão de Suporte a Serviços de TI / DTI – Diretoria de Tecnologia da Informação da Presidência
Tabela 04 – Definição dos papéis dos integrantes da contratação

A Contratada deverá enviar um e-mail ao Gestor do Contrato ou fiscal do contrato, com todas as informações necessárias para utilização do objeto da licitação.

Os telefones para contato em horário comercial junto ao gestor e fiscais do contrato são (62) 3216-4199, 3216-1190, 3216-8852 e 3216-1186.

8. PROPOSTA DE PREÇOS

Deve ser apresentada a Proposta de Preço, informando o Item, nome do objeto ofertado, fabricante/fornecedor/desenvolvedor, part-number ou identificação correlata, além do valor unitário e total para cada Item deste Termo de Referência, onde todas as despesas necessárias à perfeita execução desse projeto (fretes, seguros, taxas, impostos e demais encargos) devem estar inclusas nos preços cotados. A tabela a seguir demonstra o formato da proposta de preços:

Item	Objeto	Fabricante/Fornecedor/ Desenvolvedor/	Part-number ou identificação correlata	Qtde	Valor Unitário	Valor Total
					R$ ...	R$ …

Número do CNPJ / Razão Social:

Endereço Completo com CEP:

Fone/Fax/Celular:

E-mail:

Banco/Nome e nº da Agência/Conta-Corrente:

Prazo de Validade da Proposta:

Prazo para entrega/início da prestação dos serviços:

Local e Data:

(nome e assinatura do representante legal)

Tabela 05 – Modelo de proposta de preços

Deverá ser informado também o preposto da empresa, bem como o procedimento para acionar o chamado técnico de suporte/garantia.

Os preços contratados deverão compreender todas as despesas com mão de obra, impostos, encargos sociais e previdenciários, taxas, seguros e qualquer outra que incida ou venha a incidir sobre o objeto da presente contratação, com exceção das despesas com transporte e hospedagem dos funcionários do TJGO, que correrão por conta da própria contratante.

Juntamente com a "Proposta de Preços" supracitada a empresa proponente deverá apresentar o preenchimento da "Planilha de Requisitos Técnicos Obrigatórios" com toda a documentação comprobatória, exigida no Anexo IV do Termo de Referência, independentemente se o TJGO optar por realizar o Teste de Conformidade descrito na Seção 16 deste Termo de Referência. Tal exigência se justifica em razão da necessidade de agilidade, eficiência e transparência no processo de validação ponto a ponto dos requisitos técnicos exigidos neste Edital.

9. PLANO DE CONTRATAÇÃO/AQUISIÇÃO (ESTIMATIVA DE CONSUMO)

A expectativa do TJGO é assistir todo o seu parque computacional (aproximadamente 15 mil dispositivos) com a solução tecnológica a ser contratada. O quantitativo pode ser superior ao apresentado, sobretudo em virtude da alteração recente da Organização Judiciária do Estado de Goiás, conforme Lei nº 21.924 de 12 de maio de 2023. Por esse motivo e outros, a presente licitação tem a finalidade de Registro de Preços.

Dessa forma, a estimativa e/ou previsão de consumo ainda será ajustada à data de realização da licitação, bem como à capacidade operacional de configurar o ambiente tecnológico, a fim de evitar desperdícios e possíveis prejuízos à Administração Pública.

10. DOCUMENTOS EXIGIDOS JUNTO COM A HABILITAÇÃO

A proponente, junto com os documentos de habilitação, deverá comprovar capacitação técnico-operacional através de um ou mais atestados, expedidos por pessoa jurídica de direito público ou privado, mencionando que forneceu, de forma satisfatória, produtos e/ou serviços com características semelhantes às do objeto deste Edital.

Para isso, a LICITANTE deverá apresentar, no mínimo, 01 (um), podendo haver soma de atestados, Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove aptidão para execução do objeto da contratação, com no mínimo, 25% (vinte e cinco por cento) do quantitativo do objeto da contratação, contendo as seguintes informações:

1. Identificação do órgão ou empresa emitente com nome ou razão social, CNPJ, endereço completo, nome da pessoa responsável e função no órgão ou empresa, telefone para contato;
2. Indicação do CONTRATANTE de que foram atendidos os requisitos de qualidade e prazos requeridos (descrição, duração e avaliação dos resultados);
3. Descrição das principais características dos serviços, comprovando que a CONTRATADA executa ou executou o objeto da contratação, considerando: **o fornecimento de solução 100% em nuvem de proteção de dispositivos (utilizando tecnologia de EDR - Endpoint Detection and Response), contemplando instalação, configuração, suporte com operação assistida (24/7) e transferência de conhecimento para no mínimo 25% (vinte e cinco por cento) do total de dispositivos descritos neste Termo de Referência;**
4. Data de emissão do atestado ou da certidão;
5. Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto ao órgão ou empresa emitente).

Deverão ser apresentadas todas as informações necessárias à comprovação da legitimidade do atestado apresentado, tais como cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

Tal requisito de habilitação se justifica em virtude do expressivo vulto financeiro envolvido, bem como da necessidade de minimizar os riscos de segurança da informação oriundos da incapacidade de fornecimento por parte da empresa contratada.

O Tribunal se resguarda no direito de diligenciar junto à pessoa jurídica emitente do atestado/declaração de capacidade técnica, visando a obter informações sobre os produtos fornecidos e/ou serviços prestados, cópias dos respectivos contratos/aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

11. DAS OBRIGAÇÕES DA CONTRATADA

Responsabilidade por quaisquer danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato. A fiscalização ou o acompanhamento do contrato pela Administração não exclui ou reduz a responsabilidade do contratado.

1. Manutenção dos seus empregados devidamente identificados, devendo substituí-los imediatamente caso sejam considerados inconvenientes.

Fornecer em qualquer época, as informações e os esclarecimentos técnicos solicitados pela contratante sobre a execução dos trabalhos.

Sanar em tempo hábil todas as irregularidades apontadas pela fiscalização.

Responsabilidade por despesas decorrentes de infração praticadas por seus empregados nas instalações da Administração.

Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da contratante ou de terceiros de que tomar conhecimento em razão da execução do objeto, devendo orientar seus empregados nesse sentido.

Caso haja a necessidade de alocar equipamentos de informática de propriedade da empresa contratada nas dependências do TJGO, como notebooks, os mesmos deverão, obrigatoriamente, antes de se conectar com a rede interna, estar de acordo com as políticas de segurança interna do TJGO.

Comunicar à Administração por escrito e em tempo hábil, qualquer anormalidade que esteja impedindo a execução contratual, prestando os esclarecimentos julgados necessários.

Entregar os produtos e serviços de acordo com as características, quantidades e prazos especificados.

Tendo em vista a formulação e adoção de medidas para a conscientização e combate ao racismo e promoção da diversidade racial em todos os contratos firmados por esse Poder, a Contratada deverá promover ações internas de prevenção, conscientização e combate ao racismo junto a seus colaboradores. Estará previsto no Termo de Contrato ou instrumento equivalente cláusula que prevê tal obrigação, estando a Contratada ciente das condutas descritas e suas implicações.

12. DAS OBRIGAÇÕES DA CONTRATANTE

Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada.

Exigir o imediato afastamento de qualquer empregado ou representante da contratada, que embarace a fiscalização ou, ainda, que se conduza de modo inconveniente ou incompatível com o exercício das funções que lhe foram atribuídas.

Inspecionar, dentro dos prazos estabelecidos, os produtos e serviços fornecidos pela contratada e verificar a conformidade dos mesmos com o objeto deste Termo de Referência.

Efetuar os chamados de atendimento técnico e avaliar sua execução, promovendo as medidas cabíveis para que os produtos e serviços sejam executados em conformidade com as especificações técnicas constantes neste Termo de Referência.

Efetuar os pagamentos devidos, nas condições estabelecidas neste Termo de Referência e nos documentos que o integram.

Comunicar imediatamente a contratada via central de serviços ou ainda através de ofício, a respeito de quaisquer incidentes relacionados ao objeto deste Termo de Referência.

13. DO INADIMPLEMENTO

Pela inexecução total ou parcial do contrato, a administração poderá, garantida a defesa prévia, aplicar à contratada, segundo a extensão da falta cometida, as seguintes penalidades:

I. Advertência;

II. Multa;

III. Impedimento de licitar e contratar com a União, Estados, Distrito Federal e Municípios;

IV. Descredenciamento do sistema de cadastramento de fornecedores.

§1º. O Tribunal de Justiça, na quantificação da pena de multa, observará o seguinte:

I. multa de até 10% (dez por cento) sobre o valor do contrato, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatário em firmar o contrato, dentro de 10 (dez) dias contados da data de sua convocação;

II. multa de até 0,3% (zero vírgula três por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento ou serviço não realizado ou sobre a parte da etapa do cronograma físico de obras não cumprido;

III. multa de até 0,7% (zero vírgula sete por cento) sobre o valor da parte do fornecimento e/ou do serviço não realizado, ou sobre a parte da etapa do cronograma físico de obras não cumprida, por dia subsequente ao trigésimo;

IV. multa de até 10% (dez por cento) sobre o valor inadimplente do contrato/saldo remanescente do contrato, em caso de descumprimento parcial da obrigação.

V. Sem prejuízo das multas aplicadas, poderá a Administração, ao seu interesse, rescindir o contrato em caso de atraso superior ao sexagésimo dia sobre o fornecimento parcial ou integral do objeto ou etapa do cronograma físico da obra não cumprido, se for o caso.

VI. As multas serão descontadas de qualquer crédito da empresa contratada. Na inexistência de créditos que respondam pelas multas, a contratada deverá recolhê-las nos prazos que o Tribunal de Justiça determinar ou, quando for o caso, cobrada judicialmente.

VII. A penalidade de multa, que poderá ser aplicada cumulativamente com as demais sanções, e a sua cobrança, não isentará a obrigação de indenizar eventuais perdas e danos.

§2º. O impedimento de contratar com a União, Estados, Distrito Federal e Municípios será graduado pelos seguintes prazos:

I. 6 (seis) meses, nos casos de:

a. Aplicação de duas penas de advertência, no prazo de 12 (doze) meses, sem que o CONTRATADO tenha adotado as medidas corretivas no prazo determinado pela Administração;

b. Alteração da quantidade ou qualidade da mercadoria/materiais fornecidos.

II. 12 (doze) meses, no caso de retardamento imotivado da execução do objeto, do serviço, de suas parcelas ou do fornecimento de bens.

III. 24 (vinte e quatro) meses, nos casos de:

a. Entregar como verdadeira mercadoria falsificada, adulterada, deteriorada ou danificada;

b. Paralisação de serviço ou do fornecimento de bens sem justa fundamentação e prévia comunicação à Administração;

c. Praticar ato ilícito visando frustrar os objetivos de licitação no âmbito da administração estadual;

d. Sofrer condenação definitiva por praticar, por meio doloso, fraude fiscal no recolhimento de qualquer tributo;

e. Recusar a retirada da nota de empenho ou assinatura do contrato no prazo estabelecido, sem justa causa.

§3º. O fornecedor que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, comportar-se de modo inidôneo ou cometer fraude fiscal, será aplicada penalidade de impedimento de licitar e contratar com a União, os Estados, o Distrito Federal ou Municípios, por prazo não superior a 5 (cinco) anos, sendo descredenciado do Cadastro de Fornecedores, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, aplicadas e dosadas segundo a natureza e a gravidade da falta cometida.

§4º. O contrato, sem prejuízo das multas e demais cominações legais previstas, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados no art. 78, incisos I a XII e XVII, da Lei nº 8.666/93.

14. DA SUBCONTRATAÇÃO

É vedada a subcontratação, salvo autorização deste Tribunal.

15. FORMA DE PAGAMENTO

O pagamento será realizado da seguinte forma:

Item	Descrição	Formato	Prazos e Condições
1	Subscrição (assinatura de uso) anual da plataforma em nuvem para detecção e remediação de ataques digitais avançados por meio de inteligência artificial e análise comportamental para proteção de dispositivos.	**Parcela única** (no ato de início da cobertura do contrato, bem como no ato de início de cada ciclo de contrato renovado por 12 (doze) meses, atentando ao limite legal de 48 (quarenta e oito) meses.	Pagamento no **prazo de até 30 (trinta) dias consecutivos**, contados a partir do recebimento da Nota Fiscal ou Fatura e emissão do Termo de Recebimento Definitivo / Termo de Ateste da Nota Fiscal pela CONTRATANTE, por meio de ordem bancária, para crédito em banco, agência e conta-corrente indicados pelo contratado;
2	Serviço de suporte técnico com operação assistida e transferência de conhecimento	**Mensal** (após a emissão do Termo de Recebimento Definitivo, bem como durante cada ciclo de contrato renovado por 12 (doze) meses, atentando ao limite legal de 48 (quarenta e oito) meses. O pagamento do primeiro mês de serviço de suporte prestado, bem como do último mês do ciclo do contrato, ocorrerá no	Pagamento no **prazo de até 30 (trinta) dias consecutivos**, contados a partir do recebimento da Nota Fiscal ou Fatura e emissão do Termo de Recebimento Definitivo / Termo de Ateste da Nota Fiscal pela CONTRATANTE, por meio de ordem bancária, para crédito em banco, agência e conta-corrente indicados pelo contratado;

		formato pro rata die. Os demais meses serão pagos considerando o mês fechado (dia 1º ao 30º).	

Tabela 06 – Forma de pagamento

Demais condições:

- Para execução do pagamento, a contratada deverá fazer constar da nota fiscal correspondente, emitida, sem rasura, em letra bem legível em nome do Tribunal de Justiça do Estado de Goiás, CNPJ nº 02.292.266/0001-80, o nome do banco, o número de sua conta bancária e a respectiva agência;
- A Nota Fiscal deverá ser emitida pela própria CONTRATADA, obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e das propostas, não se admitindo Notas Fiscais emitidas com outros CNPJ, mesmo aqueles de filiais ou da matriz.
- Se a CONTRATADA utilizar nota fiscal eletrônica, deverá enviar os arquivos digitais em formato XML da NF-e para o Tribunal, por e-mail ou por meio de um sistema específico, seguindo as orientações do Gestor e/ou Fiscal do Contrato.

- Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o Tribunal de Justiça atestar a execução do objeto do contrato.
- A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio das certidões previstas no art. 29 da Lei nº 8.666, de 1993.
  - Os documentos referentes à regularidade fiscal deverão apresentar igualdade de CNPJ, ressalvando-se aquele que o próprio órgão emissor declara expressamente no referido documento que ele é válido para todos os estabelecimentos sede e filiais da contratada.

- Havendo erro na apresentação da Nota Fiscal 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;
- Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento;
- Antes de cada pagamento à contratada, será realizada consulta às certidões de regularidade fiscal para verificar a manutenção das condições de habilitação exigidas neste Termo;
  - Constatando-se a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante;

  - Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta para identificar possível suspensão temporária de

participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas;

- Não havendo regularização ou sendo a defesa considerada improcedente, o Tribunal de Justiça comunicará 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;

- Persistindo a irregularidade, serão adotadas as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa e o contraditório;

- 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 junto ao órgão correspondente;

    - Será rescindido o contrato em execução com a contratada inadimplente, salvo por motivo de economicidade ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do Tribunal de Justiça.

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

    - 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;

- Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

- EM = I x N x VP, sendo:
- EM = Encargos moratórios;
- N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
- VP = Valor da parcela a ser paga.
- I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6/100)}{365}$$

I = 0,00016438
TX= Percentual da taxa anual = 6%

16. DO TESTE DE CONFORMIDADE

O TJGO se reserva o direito de solicitar teste de conformidade da solução ofertada, previamente à adjudicação, com o intuito de comprovar as funcionalidades e requisitos técnicos da solução, caso não esteja seguro do total de atendimento da solução ofertada.

O teste de conformidade poderá ser realizado independentemente se a solução ofertada foi citada/exemplificada como "Modelo de Referência" no Anexo I do Termo de Referência e/ou foi objeto de Prova de Conceito (POC) durante a fase de Estudo Técnico Preliminar (ETP).

Caso o TJGO exija o teste de conformidade, a LICITANTE deverá disponibilizar a solução e iniciar os testes em até 03 (três) dias úteis a contar da data de convocação para o teste, não podendo estender por mais de 03 (três) dias a execução dos testes que deverão cobrir todos os requisitos técnicos obrigatórios exigidos neste Edital e seus anexos.

O horário da realização desse teste de conformidade será compreendido das 8 às 18hs, com intervalo de 1 (uma) hora para almoço (12h às 13h). As proponentes deverão ser objetivas na apresentação da solução tecnológica, sobretudo atentas ao preenchimento da Planilha de Requisitos Técnicos Obrigatórios exigida neste Anexo IV do Termo de Referência.

A comprovação deverá ser feita seguindo o padrão listado no Anexo IV deste Termo de Referência.

O TJGO realizará diligências objetivando comprovar a veracidade das informações prestadas pela LICITANTE. Caso fique caracterizada o uso inidôneo de documentos probatórios da capacidade jurídica, econômico-financeira e técnica da LICITANTE, a mesma ficará sujeita às penalidades administrativas, cíveis e penais previstas na lei.

17. VISTORIA TÉCNICA

A vistoria técnica tem como objetivo expor integralmente aos participantes da licitação a totalidade das condições em que serão executados os serviços, com destaque para o ambiente computacional físico e lógico, da infraestrutura, conectividade, configurações existentes e passíveis de integração ou alteração com a nova solução, sobre os quais a não observância poderá acarretar sérias distorções operacionais ou mesmo na formação do preço dos participantes.

Considerando a importância dos serviços a serem contratados e levando em conta a economicidade com a redução de riscos da contratação e da futura gestão contratual, considera-se a vistoria OPCIONAL na sede do TJGO, ampliando com isso a isonomia no domínio de informações relevantes para a construção de uma proposta comercial, preservando a competitividade do certame com a participação de empresas atentas, convictas e cuidadosas com os requisitos exigidos na presente licitação, por fim, diminuindo a possibilidade de entrada na competição de licitantes aventureiros, despreparados e menos cuidadosos com os requisitos que impactam diretamente suas propostas comerciais.

A vistoria pode ser realizada no formato presencial ou virtual, desde que agendada no prazo de 24 (vinte e quatro) horas de antecedência.

18. DOCUMENTOS COMPLEMENTARES

Integram este Termo de Referência os documentos relacionados a seguir, os quais estão vinculados à execução do contrato e sendo dele parte integrante, após devidamente ajustados com as informações correspondentes às partes contratantes:

- Anexo I – Características e Especificações Técnicas;
- Anexo II – Modelo de Termo de Compromisso e Sigilo;
- Anexo III – Modelo de Termo de Ciência;

- Anexo IV – Requisitos do Teste de Conformidade;
- Anexo V – Declaração de Atendimento ao Teste de Conformidade;
- Anexo VI – Termo de Vistoria Opcional.

Valdemar Ribeiro da Silva Júnior
Diretor da Divisão de Suporte a Serviços de TI

Glauco Cintra Parreira
Diretor do Núcleo de Contratos e Aquisições de TI

Anderson Yagi Costa
Diretor de Tecnologia da Informação

ANEXO I – TERMO DE REFERÊNCIA
CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO

ITEM 1 - SUBSCRIÇÃO (ASSINATURA DE USO) ANUAL DA PLATAFORMA EM NUVEM PARA DETECÇÃO E REMEDIAÇÃO DE ATAQUES DIGITAIS AVANÇADOS POR MEIO DE INTELIGÊNCIA ARTIFICIAL E ANÁLISE COMPORTAMENTAL PARA PROTEÇÃO DE DISPOSITIVOS.

Modelos de referência (exemplos de soluções compatíveis): Palo Alto Networks, CrowdStrike, SentinelOne

Observação: Será possibilitado que cada empresa licitante combine dois ou mais produtos/softwares/módulos com o objetivo de compor a solução tecnológica exigida neste Termo de Referência, desde que a console de administração da solução seja ÚNICA e 100% DISPONÍVEL EM NUVEM.

Requisitos mínimos da solução/plataforma tecnológica:

1. **Características gerais da solução:**

1.1. A console de administração deverá ser única para todos os dispositivos, independente da sua localização.

1.2. O acesso a console não deve depender de uma conexão VPN, ou seja, deve ser acessível a partir de qualquer rede com acesso à internet.

1.3. A solução deverá funcionar com instalação de agentes ou sensores únicos em cada dispositivo para prover todas as funcionalidades descritas no documento. A administração deles deverá funcionar por meio da conexão com a console de gerenciamento.

1.4. A console de administração deve estar disponível por meio de HTTPS utilizando pelo menos um dos navegadores abaixo:

1.4.1. Google Chrome;

1.4.2. Edge;

1.4.3. Firefox.

1.5. A administração da solução deverá ser totalmente em nuvem, logo, não deverá possuir ferramenta local de gerenciamento.

1.6. O gerenciamento da solução deve permitir o agrupamento de dispositivos por meio de uma seleção manual e da criação de regras para a adição automática de dispositivos seguindo, no mínimo, os seguintes critérios:

1.6.1. Endereço de IP;

1.6.2. Hostname;

1.6.3. Unidade Organizacional do Active Directory;

1.6.4. Versão do Agente;

1.6.5. Versão do sistema operacional;

1.6.6. Tipo de dispositivo.

1.7. A administração possibilitará a aplicação de políticas para grupos de dispositivos ou para dispositivos individuais.

1.8. A solução deverá possuir, duplo fator de autenticação para acesso a console. Compatível com, no mínimo, os seguintes fabricantes:

1.8.1. Azure Authenticator;
1.8.2. Google Authenticator.

1.9. A solução deverá disponibilizar um sistema de papéis delimitando as permissões e os acessos disponíveis para cada usuário dentro das funcionalidades da console de administração.

1.10. A console de administração deverá oferecer suporte a Single Sign On (SSO) com compatibilidade com pelo menos 3 opções distintas de provedor de identidade (IdP) da seguinte lista:
1.10.1. Active Directory Federation Services (AD FS);
1.10.2. Okta;
1.10.3. PingOne;
1.10.4. Azure Active Directory (Azure AD);
1.10.5. Google WorkSpace;
1.10.6. OpenID.

1.11. A console deverá apresentar, no mínimo, as seguintes visualizações para as detecções:
1.11.1. Detecções por tática;
1.11.2. Detecções por técnica;
1.11.3. Detecções por severidade de ataque;
1.11.4. Detecções por arquivo malicioso;
1.11.5. Detecções por usuário.

1.12. A console deverá apresentar, no mínimo, as seguintes visualizações para os dispositivos:
1.12.1. Dispositivos por sistema operacional;
1.12.2. Dispositivos por domínio.

1.13. A solução deve suportar a instalação de agentes ou sensores diretamente no sistema operacional de cada máquina (seja virtual ou física) ou diretamente no virtualizador. As duas formas serão aceitas.

1.14. A atualização dos sensores ou agentes deve ocorrer automaticamente, conforme uma política de atualização estabelecida na plataforma de gerenciamento, levando em consideração pelo menos as seguintes opções:
1.14.1. Atualização para uma versão específica;
1.14.2. Atualização para a versão mais recente disponível;
1.14.3. Atualização para uma versão anterior à mais recente;
1.14.4. Atualização para duas versões anteriores à mais recente;

1.15. A solução deverá proteger os dispositivos de ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia, entre outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais.

1.16. A plataforma em nuvem deverá ser atestada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os

provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes). Tal requisito se justifica por ser um mecanismo que o TJGO tem de garantir a segurança do ambiente que hospedará a solução/plataforma.

1.17. A plataforma em nuvem deverá cumprir com os requisitos exigidos no item 5 da certificação PCI-DSS V3.2 (Padrão de Segurança de Dados do Setor de Cartões de Pagamento) que lhe competem. Tal requisito se justifica por ser um mecanismo que o TJGO tem de garantir a segurança do ambiente que hospedará a solução/plataforma.

1.18. A solução deverá suportar os seguintes sistemas operacionais:

1.18.1. Windows 11;
1.18.2. Windows 10;
1.18.3. Windows 8.1;
1.18.4. Windows 7 SP1;
1.18.5. Windows Server 2022;
1.18.6. Windows Server 2019;
1.18.7. Windows Server 2016;
1.18.8. Windows Server 2012 R2;
1.18.9. Windows Server 2012;
1.18.10. Windows Server 2008 R2 SP1;
1.18.11. MacOS 11 ou superior;
1.18.12. Oracle Linux 8;
1.18.13. Oracle Linux 7;
1.18.14. Oracle Linux 6;
1.18.15. Red Hat Enterprise Linux (RHEL) 8.0 – 8.4;
1.18.16. Red Hat Enterprise Linux (RHEL) 7.4 – 7.9;
1.18.17. Red Hat Enterprise Linux (RHEL) 6.7 – 6.10;
1.18.18. SUSE Linux Enterprise (SLES).

1.19. A comunicação entre o agente a console deverá utilizar um túnel de segurança TLS criptografado utilizando certificate pinning.

1.20. A solução deverá permitir que o agente se comunique com a console de gerenciamento em nuvem por meio de um proxy.

1.21. A solução deve possibilitar a definição de lista de IPs especificas limitando o acesso a console de administração para uma rede específica.

1.22. Deve disponibilizar ferramenta de remediação remota para os administradores. Nesta ferramenta de remediação remota, a solução deve permitir a interação de, no mínimo, as seguintes ações:

1.22.1. Matar a execução de um processo;
1.22.2. Coletar diagnostico de logs;
1.22.3. Reiniciar ou desligar o dispositivo;
1.22.4. Mostrar conexões de rede.

1.23. A solução deve possibilitar a execução de scripts por meio da console de administração para responder a incidentes de forma remota.

1.24. Deve possibilitar que o administrador da solução interrompa o tráfego de rede de dispositivos classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento e/ou com uma faixa de rede específica configurada em uma política.

1.25. Os scripts pré-configurados pode se utilizar de pelo menos duas linguagens das listadas:
1.25.1. PowerShell;
1.25.2. Bash;
1.25.3. Python;
1.25.4. Zsh.

1.26. A solução deverá apresentar na console de gerenciamento, informações referentes às ameaças identificadas, fornecendo informações referentes a primeira vez que uma ameaça foi vista no ambiente e também quantos endpoints tiveram essa mesma ameaça.
1.27. A solução deverá isolar da rede do TJGO o endpoint infectado de forma automática.
1.28. A solução deve bloquear ou ser capaz de desfazer qualquer alteração do sistema relacionada a um ataque, como edições de registro, alterações de configuração etc.
1.29. Deve permitir que o acesso remoto aos usuários através de perfis de usuários criados que irão utilizar a console de gerenciamento.
1.30. Deve ser possível configurar permissões delimitadas para o acesso remoto as máquinas e somente a usuários selecionados por meio da console
1.31. Deve possibilitar que o administrador da solução interrompa o tráfego de rede de dispositivos classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento.
1.32. Deve haver registros de auditoria disponíveis para as atividades executadas durante o processo de remediação. Esses registros permitem visualizar detalhes importantes, como o usuário que se conectou ao host, o host que recebeu acesso, as linhas de comando e os argumentos executados, o tempo de duração e o início da sessão
1.33. Na instalação dos sensores ou agente da solução, elas não devem exigir a reinicialização (reboot) do computador servidor.
1.34. Deverá prover funcionalidade de recuperação automática de arquivos contra criptografia maliciosa devido a ataques do tipo ransomware;
1.35. A solução deve bloquear ou executar automaticamente a limpeza de malware sem intervenção humana, removendo alterações transitórias no sistema operacional, persistência, alterações em arquivos, tarefas, etc. Além disso, deve desfazer as alterações nos arquivos do usuário.

2. Características específicas para sistemas operacionais Microsoft Windows

2.1. A solução deve ter suporte, pelo menos, para as seguintes opções de configuração de proxy:
2.1.1. Configuração de proxy via GPO ou via integração nativa com GPO da Microsoft.
2.1.2. Proxy definido no agente.

2.2. Se um agente for configurado para usar duas ou mais configurações de proxy, essas configurações devem ser cumulativas. Isso significa que, se uma configuração de proxy não estiver disponível, o agente deverá usar o proxy definido na estação. Em último caso, se nenhum proxy estiver disponível, o agente deverá tentar estabelecer uma conexão direta.
2.3. A solução deverá possibilitar que o agente ignore qualquer configuração de proxy existente na máquina, dessa forma, deverá utilizar uma conexão direta para a console de gerenciamento em nuvem.

2.4. A solução deverá possuir métodos para remoção do agente, através de aprovação na console de gerenciamento, por uma senha ou através de um token para cada dispositivo gerenciado.
2.5. A solução deve detectar tentativas de manipulação indevida dos componentes do agente
2.6. A solução deve ser capaz de oferecer visibilidade de potenciais ataques não provenientes de arquivos e executáveis por meio de varreduras na memória e CPU.
2.7. A detecção e a prevenção de ameaças devem incorporar aprendizado de máquina (Machine Learning), de forma a permitir a personalização do nível de segurança para um determinado grupo de dispositivos ou permitir a escolha pelo administrador de quais motores de detecção serão ativados.
2.8. O sistema de aprendizado de máquina (Machine Learning - ML) deve ser capaz de detectar e prevenir tanto a execução quanto a escrita de artefatos maliciosos, sejam eles conhecidos ou desconhecidos. Isso significa que, se um binário considerado malicioso pelo motor de ML for gravado no disco, deverá ocorrer uma detecção e prevenção durante a operação de escrita no disco.
    2.8.1. Caso seja configurado para bloqueio o arquivo deverá ser quarentenado.

2.9. A solução deverá ser capaz de detectar e prevenir os seguintes tipos de ameaças:
    2.9.1. Ameaças baseadas na análise do centro de inteligência do fabricante;
    2.9.2. Scripts e comandos em Powershell considerados suspeitos;
    2.9.3. Adware;
    2.9.4. Ameaças com assinaturas/hashes de arquivos que foram adicionadas na console manualmente;
    2.9.5. Operações em registros suspeitos;
    2.9.6. Processos suspeitos.

2.10. Os agentes deverão ser capazes de detectar e de prevenir ameaças mesmo que o dispositivo não esteja conectado à internet.
2.11. A plataforma deverá permitir a quarentena de arquivos considerados maliciosos.
2.12. A solução deverá ser capaz de proteger a vulnerabilidade associada ao ASLR (Address Space Layout Randomization), proteger ou blindar.
2.13. A solução deverá impedir ataques que sobrescrevem SEH (Structured Exception Handling).
2.14. A solução deverá forçar Data Execution Prevetion (DEP) para impedir ameaças que utilizem memória para execução de códigos em região de memória não executável.
2.15. A solução deverá impedir ataques que utilizem a técnica Heap Spray Preallocation.
2.16. A solução deverá impedir ataques que explorem vulnerabilidades causadas por ponteiros nulos.
2.17. A plataforma deverá contar com a análise comportamental dos processos para proteger o ambiente de ataques avançados.
2.18. Ameaças do tipo Ransomware devem ser detectadas e prevenidas com base nos seguintes comportamentos, no mínimo:
    2.18.1. Deletar backups;
    2.18.2. Comportamento associado a processos de Cryptowall e Locky;
    2.18.3. Operações em excesso ao sistema de arquivos;
    2.18.4. Processo suspeito de deleção de um volume de “Shadow Copies”.

2.19. Ameaças com comportamento anormal deverão ser detectadas se baseando nos seguintes comportamentos:
- 2.19.1. Criação de processos suspeitos originados de navegadores;
- 2.19.2. Detecção de comprometimento de servidores Web através de webshell;
- 2.19.3. Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução;
- 2.19.4. Injeção de código não esperada de um processo a outro;
- 2.19.5. Execução de JavaScript através do executável Rundll32;
- 2.19.6. Deve ser capaz de detectar de processos que tentam comprometer credenciais de login;

2.20. A solução deverá ter sido avaliada pelo MITRE e atender ao menos as seguintes técnicas da avaliação do MITRE ATT&CK:
- 2.20.1. T1003, T1012, T1018, T1021, T1026, T1027, T1036, T1047, T1048, T1049, T1053, T1055, T1059, T1061, T1070, T1087, T1095, T1102, T1110, T1112, T1132, T1136, T1204, T1218, T1219, T1222, T1543, T1547, T1548, T1550, T1559, T1560, T1562, T1564, T1567, T1570, T1574.

2.21. A solução deverá ter sido avaliada pelo MITRE ATT&CK Engenuity (https://attackevals.mitre-engenuity.org/enterprise/participants) para no mínimo os adversários abaixo:
- 2.21.1. APT3;
- 2.21.2. APT29;
- 2.21.3. Carbanak + FIN7;
- 2.21.4. Wizard Spider + Sandworm.

2.22. Na console de gerenciamento, as detecções devem ser contextualizadas pela matriz do MITRE ATT&CK, mostrando os objetivos, táticas e técnicas que foram observadas no evento.

2.23. O agente para estações de trabalho Windows deve suportar RFC 5246.

2.24. Deve possibilitar que a proteção de dispositivos seja habilitada em modo de detecção, sem tomada de ação efetiva, ou possuir algum mecanismo de bloqueio que possa evitar a indisponibilidade massiva dos dispositivos, sobretudo na época da implantação da solução.

2.25. A solução deve permitir bloqueio de dispositivos USB baseado em, no mínimo, as seguintes classes de dispositivos:
- 2.25.1. Dispositivos de imagem;
- 2.25.2. Dispositivos de áudio e vídeo;
- 2.25.3. Dispositivos móveis;
- 2.25.4. Impressoras;
- 2.25.5. Adaptadores de rede wireless;
- 2.25.6. Dispositivos de armazenamento em massa. Para os dispositivos de armazenamento em massa, deve atribuir, no mínimo, as seguintes permissões granulares:
  - 2.25.6.1. Somente leitura;
  - 2.25.6.2. Escrita e leitura;
  - 2.25.6.3. Bloqueio total.

2.26. O controle de dispositivos USB deve permitir exceções baseadas em VendorID e ProductID, número serial e classe.

3. Características específicas para sistemas operacionais MAC

3.1. Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e bloqueios de ataques ou ações maliciosas;
3.2. A detecção e a prevenção de ameaças devem incorporar aprendizado de máquina (Machine Learning), de forma a permitir a personalização do nível de segurança para um determinado grupo de dispositivos ou permitir a escolha pelo administrador de quais motores de detecção serão ativados;
3.3. Deve ser capaz de detectar Adware e programas potencialmente indesejados;
3.4. Deve ser capaz de detectar ameaças mesmo que o dispositivo não esteja conectado à Internet;
3.5. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;
3.6. Deve permitir bloqueio automático de processos suspeitos;
3.7. Deve permitir bloqueio baseado em análise do centro de inteligência do fabricante;
3.8. Deve permitir que arquivos possam ser movidos para uma área de quarentena;
3.9. Deve permitir bloqueio de utilização suspeita do modelo XPCOM;
3.10. Deve permitir bloqueio de processos que se assimile ao comportamento do backdoor Empyre;

4. Características específicas para sistemas operacionais Linux

4.1. Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção de ataques;
4.2. A detecção e a prevenção de ameaças devem incorporar aprendizado de máquina (Machine Learning), de forma a permitir a personalização do nível de segurança para um determinado grupo de dispositivos ou permitir a escolha pelo administrador de quais motores de detecção serão ativados;
4.3. Deve permitir níveis de sensibilidade diferentes ou definir quais motores serão utilizados para detecção e prevenção de ataques através do componente de aprendizado de máquina;
4.4. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;
4.5. Deve permitir bloqueio de processos com comportamento malicioso de acordo com a inteligência da fabricante;
4.6. Deve permitir monitorar as atividades e eventos relacionadas a rede;
4.7. Deve permitir monitorar as atividades e eventos relacionadas a sistemas de arquivo;
4.8. Deve permitir monitorar as atividades e eventos relacionadas a tráfego não encriptado TLS.

5. Capacidades de inteligência de ameaças

5.1. A solução deverá possuir feeds de inteligência, capaz de compartilhar globalmente ameaças identificadas com os clientes, a fim de realizar a prevenção de ataques no ambiente do TJGO.
5.2. A inteligência de ameaças deve mapear campanhas de ataque e dar visibilidade de países e indústrias alvo, pais de origem da campanha e última atividade;
5.3. Para as campanhas de ameaças, a inteligência de ameaças deve fornecer, quando aplicável, informações como as vulnerabilidades utilizadas, os métodos de entrega, uma breve

descrição da campanha, a forma de monetização, os métodos de ataque e a motivação por trás da campanha;

5.4. Deve permitir extrair indicadores de comprometimento, como por exemplo, hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de email, nomes de arquivos associados às atividades maliciosas.

6. Capacidade de Firewall Local em sistemas operacionais Windows e Mac

6.1. Deve permitir a criação de regras, grupos de regras e políticas de firewall para definir com precisão qual tráfego de rede é permitido e bloqueado no host;

6.2. A política de firewall deve permitir a utilização de múltiplas regras de firewall;

6.3. As regras de firewall devem ser agrupáveis, ou seja, as regras de firewall utilizadas em uma política devem ser configuradas de forma a ser possível de selecionar um grupo de regras a serem usadas em uma política;

6.4. Regras de firewall devem suportar minimamente as seguintes características:

6.4.1. IPv4;

6.4.2. IPv6;

6.5. Protocolos:

6.5.1. TCP;

6.5.2. UDP;

6.5.3. ICMP;

6.5.4. Avançado (permitindo especificar o número do protocolo).

6.6. Endereço local;

6.6.1. Porta local;

6.6.2. Endereço remoto;

6.6.3. Porta remota;

6.7. Ação:

6.7.1. Permitir;

6.7.2. Bloquear.

6.8. Direção da conexão:

6.8.1. Inbound;

6.8.2. Outbound;

6.8.3. Inbound ou Outbound.

6.9. Perfil de rede (para que a regra seja aplicada de acordo com):

6.9.1. Rede LAN;

6.9.2. Rede WLAN.

6.10. Deve ser possível a configuração de regras de firewall para permitir ou negar (Allow and Deny);

6.11. As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente.

6.12. A Solução deve possibilitar a aplicação de regras de firewall personalizadas dependendo da localização de rede do dispositivo.

6.13. A solução deverá trabalhar com localização permitindo as seguintes funcionalidades:

6.13.1. IP Address;

6.13.2. DNS Server.

7. Capacidades de emulação de execução de código (Sandbox)

7.1. A solução deve prover, integrada à console de administração, capacidades de emulação de execução de arquivos;

7.2. Deve se integrar ao agente instalado em dispositivos para permitir que arquivos suspeitos sejam enviados de forma automática ao serviço de emulação de execução;

7.3. A solução deve emular execução, no mínimo, nos seguintes sistemas operacionais:

7.3.1. Windows

7.3.2. Linux

7.4. A solução deve incluir na análise de execução, no mínimo, as seguintes características:

7.4.1. Táticas e técnicas de acordo com o framework do MITRE ATT&CK;

7.4.2. Caraterísticas comportamentais suspeitas;

7.4.3. Detalhes do arquivo como nome, hash, tamanho, tipo;

7.4.4. Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;

7.4.5. Atividades de arquivos;

7.4.6. Detalhes de processos iniciados durante a execução.

8. Relatórios e dashboard

8.1. A solução deve fornecer um dashboard que exiba as detecções, o número de novas detecções e as detecções por tipos de ameaças, por pelo menos, os últimos 30 dias.

8.2. A plataforma deverá ter a capacidade de reportar as detecções de forma agrupada das seguintes formas:

8.2.1. Por dispositivo afetado;

8.2.2. Por técnica;

8.2.3. Por tática;

8.2.4. Por arquivo detectado;

8.2.5. Por linha de comando;

8.2.6. Por severidade.

8.2.7. A plataforma deverá ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.

8.2.8. A plataforma deverá ter a capacidade de reportar as detecções, permitindo filtrar minimamente com base aos seguintes filtros:

8.2.9. Detectadas na última hora;

8.2.10. Detectadas na última semana;

8.2.11. Detectadas no último dia;

8.2.12. Detectadas nos últimos 30 dias;

8.2.13. Hash;

8.2.14. Host;

8.2.15. Nome de arquivo;

8.2.16. Severidade;

8.2.17. Linha de comando;

8.2.18. Tática;

8.2.19. Técnica;

8.2.20. Tipo de sistema operacional;

8.2.21. Usuário;

8.2.22. Versão do sistema operacional.

8.3. A solução deve prover a capacidade de relatório de todas as conexões remotas realizadas por meio da console de gerenciamento ao endpoint gerenciado contendo informações que não deverão ser passiveis de exclusão ou limpeza, garantindo o não repúdio das informações apresentadas.

8.4. A plataforma deverá gerar relatório das máquinas contendo minimamente as seguintes informações, podendo ser exportada em CSV:
- 8.4.1. Data e hora da primeira comunicação;
- 8.4.2. Data e hora da última comunicação;
- 8.4.3. Hostname;
- 8.4.4. Identificação do host (UID/GUID);
- 8.4.5. IP local da máquina;
- 8.4.6. IP público da máquina;
- 8.4.7. MAC Address;
- 8.4.8. Política de atualização aplicada;
- 8.4.9. Política de controle de dispositivos USB aplicada;
- 8.4.10. Política de proteção aplicada;
- 8.4.11. Site;
- 8.4.12. Tipo;
- 8.4.13. Unidade organizacional (OU);
- 8.4.14. Versão do sensor/agente instalado.
- 8.4.15. Versão do sistema operacional;

8.5. O relatório de máquinas deverá ter a capacidade de aplicar filtros para inclusão ou exclusão de dados no relatório, considerando minimamente as seguintes opções de filtro:
- 8.5.1. Domínio;
- 8.5.2. Grupo;
- 8.5.3. Hostname;
- 8.5.4. Identificação do host (UID/GUID);
- 8.5.5. IP local da máquina;
- 8.5.6. MAC Address;
- 8.5.7. Plataforma;
- 8.5.8. Política de atualização aplicada;
- 8.5.9. Política de proteção aplicada;
- 8.5.10. Subnet da máquina;
- 8.5.11. Unidade organizacional (OU);
- 8.5.12. Versão do sensor/agente instalado;
- 8.5.13. Versão do sistema operacional.

8.6. Deverá apresentar a lista de dispositivos gerenciados com a capacidade de filtro baseado minimamente nas seguintes categorias:
- 8.6.1. Por endereço de IP;
- 8.6.2. Por nome do Site;
- 8.6.3. Por plataforma do Sistema Operacional;
- 8.6.4. Por Status do host;
- 8.6.5. Por tipo do Sistema Operacional;
- 8.6.6. Por unidade organizacional do host;

8.6.7. Por versão do Sistema Operacional;

8.7. Workflows e notificações

8.7.1. A solução deve suportar utilização e criação de workflows para automatização e definição de ações para administração da solução e automatização de respostas em função de detecções encontradas e consideradas importantes.

8.7.2. A solução deve possibilitar a utilização de workflows de automatização a partir de playbooks pré configurados para cenários específicos.

8.7.3. Deve suportar no mínimo os seguintes gatilhos de início do workflow:

8.7.3.1. Nova detecção;

8.7.3.2. Detecção atribuída a um usuário para investigação;

8.7.3.3. Política criada;

8.7.3.4. Política deletada;

8.7.3.5. Política habilitada;

8.7.3.6. Política desabilitada;

8.7.3.7. Política atualizada.

8.8. Deve permitir a configuração das seguintes ações tomadas automaticamente:

8.8.1. Conter a rede do dispositivo, fazendo que ele só se comunique com a console da solução;

8.8.2. Pegue o arquivo associado a uma detecção da endpoint e faça o upload para a console;

8.8.3. Remova o arquivo associado a uma detecção do endpoint;

8.8.4. Notifique um usuário.

8.9. A solução deve possibilitar a configuração de pelo menos o seguinte canal de notificação no workflow:

8.9.1. E-mail.

9. Planejamento e implantação da solução tecnológica (subscrições)

9.1. Após a assinatura do contrato, uma reunião inicial de alinhamento deverá ocorrer, em até 3 (três) dias úteis, a fim de que sejam apresentadas as equipes técnicas de trabalho e gestão/fiscalização do contrato, bem como viabilizada a assinatura do Termo de Compromisso e Sigilo de Informações.

9.2. A CONTRATADA deverá elaborar um Plano de Implantação da solução tecnológica, em até 8 (oito) dias úteis após a assinatura do contrato. Esse Plano será objeto de análise e aprovação da equipe técnica da CONTRATANTE. A aprovação desse Plano pelo TJGO ocorrerá em no máximo 2 (dois) dias úteis. Os serviços de implantação somente serão iniciados mediante aprovação da CONTRATANTE.

9.3. O prazo para instalação e configuração da solução/plataforma tecnológica, bem como a integração com os dispositivos necessários a serem protegidos (quantidade estipulada no contrato), será de no máximo de **45 (quarenta e cinco) dias corridos** contados da data de assinatura do contrato. Nesse prazo, já estão incluídas as **reuniões iniciais de planejamento, entrega das subscrições, aprovação do Plano de Implantação e demais tratativas.**

9.4. <u>O prazo de vigência das licenças (subscrições) será contabilizado a partir da entrega/ativação das licenças na console de gerência.</u>

9.5. As atividades de instalação e configuração relacionadas ao ITEM 1, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno e/ou finais de semana, mediante acordo entre a equipe técnica do TJGO e a CONTRATADA. Não havendo acordo, permanece a necessidade/regra de cumprimento das atividades de instalação e configuração dentro do horário comercial.

9.6. Nos casos de atuações remotas, a CONTRATADA deverá pré-agendar com a equipe do TJGO os horários para os acessos necessários de acordo com as políticas e diretrizes de segurança do TJGO.

9.7. Nesta etapa o TJGO não disponibilizará qualquer infraestrutura de hardware e/ou software, apenas parte da equipe técnica do TJGO acompanhará a ativação dos serviços e da console de administração, bem como a integração com os dispositivos do TJGO, mantendo sempre o alinhamento com a Política de Segurança da Informação do TJGO.

9.8. O ITEM 1 só será aceito definitivamente mediante a conclusão dessa etapa de Implantação. Momento então que começará a ser prestado o serviço de suporte técnico com operação assistida previsto no ITEM 2.

ITEM 2 - SERVIÇO DE SUPORTE TÉCNICO COM OPERAÇÃO ASSISTIDA E TRANSFERÊNCIA DE CONHECIMENTO

Requisitos mínimos do serviço a ser contratado:

1. Do serviço de suporte técnico com operação assistida

1.1. A CONTRATADA deverá fornecer suporte direto do fabricante da solução durante toda a vigência contratual para atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante se necessário, além do nível de suporte que deverá ser prestado pela CONTRATADA em conjunto.

1.2. Os atendimentos deverão ser do tipo telefônico, internet, e-mail e/ou chat, no formato 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, e deverá ser realizado por profissionais especializados, sendo necessário cobrir todo e qualquer defeito ou demanda apresentada.

1.3. Os serviços de suporte e manutenção também consistem em atendimentos a dúvidas técnicas quanto ao uso do ambiente e atualizações de versões para correções de eventuais problemas identificados.

1.4. As atividades de suporte técnico serão realizadas, a critério do TJGO, em seu ambiente tecnológico, a partir da assinatura do Contrato e durante toda sua vigência contratual.

1.5. O suporte técnico poderá ser utilizado para melhoria das configurações do ambiente tecnológico, continuidade do processo de implantação e integração dos dispositivos e desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

1.5.1. Orientação sobre acesso, o uso, a configuração, a instalação de agentes e/ou sensores nos dispositivos do TJGO, contando com acesso ao conhecimento privilegiado de recursos da CONTRATADA e quando necessário do FABRICANTE da solução.

1.5.2. Orientação quanto às melhores práticas para implementação e integração da solução no ambiente do TJGO.

1.5.3. Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução e seu impacto nos agentes e/ou sensores já instalados no ambiente do TJGO.

1.5.4. Análise técnica qualificada nas análises e prevenções de vulnerabilidades encontradas e passíveis de serem exploradas nos dispositivos protegidos e monitorados pela console central.

1.5.5. Aplicação de melhores práticas para implementação dos produtos de software adquiridos;

1.5.6. Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático caso aconteçam.

1.5.7. Realização de estudos para melhoria do ambiente atual, políticas, prevenções, análises e aumento da proteção para diminuição e mitigação de vulnerabilidades encontradas.

1.5.8. Implementação de novas integrações que não tenham ainda sido efetivadas ou sejam necessárias novas integrações.

1.5.9. Identificação de melhorias e respectivo tratamento (melhoria de parametrização).

1.5.10. Parametrização da solução, de acordo com as regras e políticas disponíveis em sua console única e definidas pelo TJGO.

1.5.11. Apoio para execução de procedimentos de atualização para novas versões dos agentes e/ou sensores instalados nos dispositivos.

1.5.12. Apoio à elaboração e adequação de relatórios executivos, gerenciais e operacionais quando necessário.

1.5.13. Suporte avançado para estratégia e planejamento de migrações e adequações nos agentes e sensores instalados nos dispositivos protegidos pela solução.

1.5.14. Avaliação e comparação de novas funcionalidades de forma remota e se necessário presencial, mediante solicitação prévia da equipe do TJGO.

1.5.15. Apoio quanto a obstáculos operacionais e de planejamento, incluindo, sem limitação, a configuração dos componentes da solução, problemas de usabilidade, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes.

1.6. Os serviços poderão ser prestados de forma remota observando as seguintes condições:

1.6.1. O suporte poderá ser prestado por telefone, e-mail, chat ou internet, prioritariamente serão abertos os chamados via e-mail.

1.6.2. Durante as sessões remotas a CONTRATADA deverá utilizar ferramenta própria para acesso remoto seguro (exemplo: Bomgar, LogMeIn) ao ambiente do TJGO, possibilitando a gravação da sessão e possibilitando o acesso simultâneo de todos os envolvidos na solução do chamado, seguindo todas as diretrizes de segurança pré-estabelecidas.

1.6.3. O sistema deverá permitir abertura de chamados via telefone, e-mail e/ou console de acesso web pela equipe do TJGO.

1.6.4. Em casos de chamados abertos via telefone, o sistema deverá disponibilizar um número 0800 ou um número local onde o TJGO possui sua sede (Goiânia-GO), neste último caso, o número deverá ser disponibilizado pela CONTRATADA no formato (062) + (número local). Deverá ainda possibilitar a abertura de chamados por meio de gravação de áudio, caso os atendentes estejam ocupados no momento da ligação, devendo o sistema identificar o número utilizado pré-cadastrado e liberado para abertura de chamados que serão automaticamente abertos e enviados para uma fila de atendimentos apropriada, devendo registrar o horário do momento da ligação como horário de abertura do chamado em questão.

1.6.5. Não haverá limite para o número de chamados de suporte técnico.

1.6.6. O nível de severidade será atribuído pela equipe autorizada do TJGO no momento da abertura do chamado.

1.6.7. Durante os atendimentos dos chamados, para efeitos de apuração do tempo despendido para solução, serão desconsiderados os períodos em que o TJGO estiver responsável por executar alguma ação necessária para a análise e solução da ocorrência ou quando for necessário aguardar alguma correção por parte do fabricante que não impacte no funcionamento e utilização do ambiente, sendo permitido nestes casos pausar ou interromper o chamado, mas sem alterar o número inicial de protocolo/número de abertura do mesmo.

1.6.8. Uma vez que a solução estará em produção e funcionando em nuvem, as atividades relacionadas a correções ou atualizações da console que necessitarem indisponibilidade do ambiente, sem prejuízo para o funcionamento dos dispositivos já gerenciados pela solução, deverão ser notificadas o TJGO com antecedência mínima de 1 (um) dia útil.

1.6.9. Para chamados de severidade Urgente/Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

Severidade	Descrição	Prazo máximo de início de atendimento remoto	Prazo máximo da solução
Urgente/Crítica Severidade 1	Situação emergencial ou problema crítico que cause indisponibilidade do ambiente.	Até 2 (duas) horas após a abertura do chamado remoto.	Até 72 (setenta e duas) horas após abertura do chamado remoto.
Alta Severidade 2	Impacto de alta significância relacionado à utilização do ambiente: ocorrência de indisponibilidade de funcionalidade ou recurso importante onde as operações continuam de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Até 4 (quatro) horas após a abertura do chamado remoto.	Até 5 (cinco) dias corridos após abertura do chamado remoto.
Normal Severidade 3	Impacto de baixa significância relacionado à utilização do ambiente. Não há ocorrência de indisponibilidade de funcionalidade ou recurso, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 8 (oito) horas após a abertura do chamado remoto.	Até 8 (oito) dias corridos após abertura do chamado remoto.
Baixa Severidade 4	Consulta e/ou dúvida técnica e/ou transferência de conhecimento	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	Até 10 (dez) dias corridos após a abertura do chamado remoto.

1.7. O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação de advertências formais e caso seja definido pelo TJGO poderão ser aplicadas glosas conforme tabela a seguir e serem descontadas da garantia financeira dos serviços prestados:

Resultado esperado e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da glosa	Limite da glosa
Urgente/Crítica	1 hora	NHA * 0,05 * VMS	50% da VMS
Alta	1 hora	NHA * 0,03 * VMS	50% da VMS
Normal	1 hora	NHA * 0,01 * VMS	50% da VMS
Baixa	1 hora	NHA * 0,005 * VMS	50% da VMS

Onde:
NHA = Número de horas de atraso após o término do prazo máximo esperado para solução.

VMS = Valor mensal do suporte.

1.8. Durante o período de vigência do contrato a CONTRATADA deverá apresentar mensalmente relatório em formato eletrônico, contendo todos os chamados ocorridos no mês e seus prazos de atendimento, contendo informações analíticas e sintéticas de cada chamado, contendo a lista e total de chamados concluídos dentro e fora do prazo de SLA estabelecido;

1.9. Deverá ser garantido ao TJGO pleno acesso ao site do FABRICANTE, além de acesso irrestrito a console de gerenciamento da solução em nuvem, devendo ser possível delegar a função de abertura de chamados com o FABRICANTE para a CONTRATADA, assim

como delegar os acessos necessários para a execução dos serviços de suporte diretamente pela equipe da CONTRATADA.

2. Transferência de conhecimento na solução

2.1. O TJGO poderá solicitar durante toda a vigência contratual do serviço, transferência de conhecimento e/ou operação assistida de segunda a sexta-feira em horário comercial como parte integrante do serviço prestado, para isso poderá ser solicitado sessões remotas e/ou presenciais, bem como workshops de transferência de conhecimento para a equipe técnica, para isso serão abertos chamados com severidade “4” classificado como “Baixa”.

2.2. As transferências de conhecimento poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverá ser realizado nas dependências do TJGO, com instrutor certificado na solução e deverá ter carga horária mínima de 04 (quatro) horas, e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério do TJGO, de modo que os alunos possam absorver os conhecimentos oficiais do fabricante acerca da solução fornecida, sendo todos os custos de deslocamento do instrutor e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA.

2.3. As capacitações virtuais deverão ser oficiais do fabricante da solução, através de plataforma virtual de capacitação (textos, vídeos, tutoriais, laboratório de simulação, testes de aprendizado) na modalidade EAD (Ensino a Distância), no idioma português do Brasil (preferencialmente) ou inglês.

2.4. A plataforma virtual de capacitação deve permitir capacitação simultânea para pelo menos 10 (dez) profissionais do TJGO. Não será formada turma com mais de 20 profissionais do TJGO.

2.5. Para os casos em que for necessária a forma presencial, o prazo de início será estipulado pela equipe do TJGO, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo, multa ou glosa para a CONTRATADA.

2.6. Inicialmente, quando da assinatura do contrato, serão solicitadas, no mínimo, 2 (duas) workshops de transferência de conhecimento, sendo:

2.6.1. a primeira, na época da implantação da solução, para possibilitar a transferência de conhecimento para toda a equipe técnica do TJGO em tempo de execução com a solução funcionando;

2.6.2. a segunda, quando a solução estiver em produção e devidamente integrada ao ambiente no TJGO.

2.7. Além da previsão do requisito no item anterior (2.6), o TJGO poderá solicitar no máximo 1 (uma) workshop de transferência de conhecimento por semestre, caso a equipe do TJGO entenda que seja necessário, durante toda a vigência do contrato.

2.8. A transferência deverá garantir, pelo menos, acesso aos seguintes tópicos:

2.8.1. Visão geral da solução;
2.8.2. Fundamentos e configurações da solução;
2.8.3. Instalação dos sensores e troubleshooting;
2.8.4. Administração de Dashboards;
2.8.5. Administração do firewall no endpoint;
2.8.6. Utilização do MitreAtt&ck;
2.8.7. Fundamentos de Investigação;
2.8.8. Fundamentos de Threat Intelligence;
2.8.9. Investigação baseado em Sandbox;
2.8.10. Resposta em Real Time;

2.8.11. Fundamentos na avaliação de incidentes;
2.8.12. Fundamentos da arquitetura Zero Trust.

2.9. Os servidores participantes farão avaliação da capacitação (transferência de conhecimento) com atribuição de grau, conforme indicado abaixo:
2.9.1. I (insatisfatório) – 0 a 25%
2.9.2. R (regular) – 25 a 50%
2.9.3. B (bom) – 50 a 75%
2.9.4. MB (muito bom) – 75 a 100%

2.10. O gestor do contrato atestará/aceitará a capacitação (transferência de conhecimento) realizada, se no mínimo 60% das avaliações indicarem os graus B (bom) e/ou MB (muito bom).

ANEXO II – TERMO DE REFERÊNCIA
MODELO DE TERMO DE COMPROMISSO E SIGILO

O <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n.°<CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.°<CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;
Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e os Decretos nº 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO

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

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

A vigência deste Termo independe do prazo de vigência do contrato assinado.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo

CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, a CONTRATADA assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do CONTRATANTE.

Parágrafo Quarto – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados 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, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das

Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro da <CIDADE DO CONTRATANTE>, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.
E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

_____, _____ de _____ de 20____

De acordo.

CONTRATANTE	CONTRATADA
_____	_____
<Nome> Matrícula: <Matr.>	<Nome> <Qualificação>

Testemunhas

_____	_____
<Nome> <Qualificação	<Nome> <Qualificação

ANEXO III – TERMO DE REFERÊNCIA
MODELO DE TERMO DE CIÊNCIA

Contrato Nº			
Objeto			
Contratante			
Gestor do Contrato		Matrícula	
Contratada		CNPJ	
Preposto da Contratada		CPF	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes no Contratante.

Goiânia,_____ de _____de _____

Ciência

CONTRATADA	
Funcionários	
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>

ANEXO IV – TERMO DE REFERÊNCIA
REQUISITOS DO TESTE DE CONFORMIDADE

A comprovação dos requisitos técnicos obrigatórios deverá utilizar a planilha modelo abaixo e deverão ser demonstrados e comprovados pela LICITANTE melhor classificada no certame, no teste de conformidade, obrigatoriamente em tempo de execução com o ambiente em funcionamento na nuvem da LICITANTE e poderá ser realizado de forma remota. Será de responsabilidade e as expensas da LICITANTE, a disponibilização de todo aparato necessário (softwares e hardwares) para a execução dos testes.

Será exigida a comprovação de todos os requisitos técnicos obrigatórios listados e exigidos neste edital na DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO.

As LICITANTES deverão, para cada requisito exigido, declarar se atende ou não ao requisito. A comprovação deverá ser feita através de manuais, folhetos, ou prospectos autorizados e produzidos pelo fabricante da solução, que deverão ser entregues, devidamente numerados e ordenados para consulta pela equipe do TJGO, juntamente com a planilha de requisitos técnicos obrigatórios, além da demonstração em tempo de execução para a equipe de homologação do teste de conformidade do TJGO.

A Planilha de requisitos técnicos obrigatórios deverá ser entregue, devidamente preenchida e assinada pela LICITANTE, acompanhada de toda documentação comprobatória, juntamente com a proposta comercial no momento de cadastramento da mesma e da documentação de habilitação no site e-licitações.

Ficam estabelecidas as seguintes definições para determinação da forma de atendimento a cada requisito:

O ambiente para o teste de conformidade deverá disponibilizado e estar em pleno funcionamento com todas as características necessárias, sem nenhum custo adicional para a TJGO, para isso a LICITANTE deverá observar na VISTORIA TÉCNICA prévia descrita neste projeto, e deverá cumprir o prazo máximo de até 03 (três) dias úteis a contar da data de convocação para o teste, não podendo estender por mais de 02 (dois) dias a execução dos testes que deverão cobrir todos os requisitos técnicos obrigatórios exigidos neste Edital e seus anexos.

Para TODOS os requisitos a LICITANTE deverá demonstrar o atendimento imediatamente no teste de conformidade para a equipe da TJGO, sujeito a desclassificação quando da não demonstração ou não atendimento de qualquer um dos requisitos.

A LICITANTE será comunicada quando deverá proceder a disponibilização do ambiente para o teste de conformidade. Caso o ambiente não esteja em pleno funcionamento com todos requisitos técnicos exigidos no prazo determinado, a LICITANTE será considerada desclassificada, sendo chamada a próxima colocada e assim por diante.

Uma vez atendidos e demonstrados todos os requisitos técnicos obrigatórios, a TJGO emitirá Declaração de atendimento conforme listado no Anexo V do Termo de Referência.

PLANILHA DE REQUISITOS TÉCNICOS OBRIGATÓRIOS

Requisito	Descrição	Atendido (Sim ou Não)	Nome do Manual	Referência à página e título na documentação comprobatória	Trecho da comprovação
1					
2					
3					
4					

ANEXO V – TERMO DE REFERÊNCIA
DECLARAÇÃO DE ATENDIMENTO AO TESTE DE CONFORMIDADE

DEMONSTRAÇÃO DO TESTE DE CONFORMIDADE DOS REQUISITOS FUNCIONAIS DO AMBIENTE

DECLARAMOS, para fins de instrução de processo licitatório do TJGO, que a empresa _____, por meio de seu Responsável Técnico, inscrita no CNPJ sob o no _____, atendeu, demonstrou, e comprovou, todos os requisitos do teste de conformidade conforme listado no ANEXO IV.

Declaramos ainda que toda demonstração foi realizada e acompanhada pela equipe do TJGO.

_____

Assinatura do responsável da LICITANTE

_____

Assinatura do representante do TJGO

ANEXO VI – TERMO DE REFERÊNCIA
TERMO DE VISTORIA OPCIONAL

Declaro, para fins de convalidação do domínio de informações relevantes para a participação no Pregão Eletrônico nº ____/2023, que vistoriei o ambiente e parque tecnológico do TJGO onde serão prestados os serviços e integrados os dispositivos a serem protegidos pela solução.

Declaro que estiveram a minha disposição todas as informações necessárias, inclusive as que requisitei para a identificação dos serviços, das condições e dos requisitos licitatórios, tendo sido sanada pela equipe técnica dos órgãos, todas as dúvidas que foram por mim apresentadas e questionadas.

Declaro, sob as responsabilidades impostas pela legislação vigente, que a empresa que represento participará da fase de lances exclusivamente na convicção de que cumpre as exigências expressas no Edital.

Declaro ainda, que será mantido por mim o sigilo de todas as informações e documentos conhecidos nesta Vistoria, cuidando para que no repasse destas informações a outrem, admitido exclusivamente para formulação de preço e condições de execução, o mesmo compromisso seja firmado formalmente.

Goiânia (GO), ____de_____de 2023

_____

Empresa Licitante

Data, nome, assinatura do responsável pela Visita Técnica e CNPJ da Empresa

_____

TJGO

Data, nome e assinatura autorizada

ASSINATURA(S) ELETRÔNICA(S)

Tribunal de Justiça do Estado de Goiás
Para validar este documento informe o código 717272496305 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

Nº Processo PROAD: 202303000392278 (Evento nº 82)

GLAUCO CINTRA PARREIRA
ANALISTA JUDICIÁRIO
NUCLEO DE CONTROLE DE CONTRATOS E AQUISIÇOES - NCCA
Assinatura CONFIRMADA em 08/08/2023 às 10:28

MARCUS VINICIUS GONZAGA FERREIRA
ANALISTA JUDICIÁRIO
DIVISÃO DE SUPORTE A SERVIÇOS DE TI - DSSTI
Assinatura CONFIRMADA em 08/08/2023 às 14:35

ANDERSON YAGI COSTA
DIRETOR DE TECNOLOGIA DA INFORMAÇÃO
SECRETARIA EXECUTIVA DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO - PRESIDÊNCIA
Assinatura CONFIRMADA em 08/08/2023 às 15:48