

Última atualização 15/10/2024

Local: Goiânia/GO **Órgão:** CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE GOIAS **Unidade compradora:** 926864 - CONSELHO REGIONAL DE CONTABILIDADE - GO**Modalidade da contratação:** Dispensa **Amparo legal:** Lei 14.133/2021, Art. 75, II **Tipo:** Aviso de Contratação Direta **Modo de disputa:** Dispensa Com Disputa**Registro de preço:** Não**Data de divulgação no PNCP:** 15/10/2024 **Situação:** Divulgada no PNCP **Data de início de recebimento de propostas:** 15/10/2024 10:19 (horário de Brasília)**Data fim de recebimento de propostas:** 18/10/2024 07:59 (horário de Brasília)**Id contratação PNCP:** 01015676000111-1-000086/2024 **Fonte:** Compras.gov.br**Objeto:**

Contratação de empresa especializada na cessão de uso de 56 licenças antivírus e sua implementação, instalação, reconfiguração e análise por 3(três) anos de uso.


Informação complementar:

Não alcançou o limite de dispensa, conforme o art. 75, inciso II.

VALOR TOTAL ESTIMADO DA COMPRA

R\$ 24.451,97

[Itens](#) [Arquivos](#) [Histórico](#)

Número	Descrição	Quantidade	Valor unitário estimado	Valor total estimado	Detalhar
1	Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software	1	R\$ 24.451,97	R\$ 24.451,97	

Exibir: 1-1 de 1 itens

Página

[< Voltar](#)

Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o sítio eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novel diploma.

É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e correteza das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

 <https://portaldeservicos.economia.gov.br> 0800 978 9001

AGRADECIMENTO AOS PARCEIROS



AVISO DE DISPENSA DE LICITAÇÃO –PROCESSO 9079602110000085.000007/2024-68

O Conselho Regional de Contabilidade de Goiás, em conformidade com o Art. 75, Inciso II – da Lei Federal nº14.133/2021 e Instrução Normativa nº 67/2021, torna público a manifestação de interesse da Administração em obter propostas adicionais de eventuais interessados para CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA AQUISIÇÃO DE DIREITO DE CESSÃO DE USO DE LICENÇA DE SOLUÇÃO DE ANTIVIRUS PARA 56 DISPOSITIVOS PARA 36(TRINTA E SEIS) MESES, ALÉM DA SUA IMPLEMENTAÇÃO, IMPLANTAÇÃO, INSTALAÇÃO, RECONFIGURAÇÃO E ANÁLISE., podendo eventuais interessados apresentarem, eletronicamente, propostas de Preços no prazo de no mínimo 3 (três) dias úteis a contar desta data de Publicação, nos termos do artigo 75, § 3º da Lei Federal nº 14.133/21, oportunidade em que a administração escolhera a mais vantajosa, após disputa on line, e após habilitação da(s) classificada(s) em primeiro lugar no item.

LIMITE PARA CADASTRO DE PROPOSTA DE PREÇOS 15/10/2024 A 18/10/2024 ÀS 08:04H.

As Proposta de Preços deverão ser publicadas na plataforma: comprasnet.gov.br, em campo próprio até a data limite.

O Aviso de Dispensa de Licitação e Termo de Referência de dispensa em anexo.

Outras informações poderão ser obtidas no Departamento de Licitações e Compras, sito a Rua 107 nº 151, Setor Sul, Goiânia, Goiás. No horário das 08:00 às 17:00 horas de segunda a sexta feira ou através do e-mail Institucional: operacional1@crcgo.org.br



Documento assinado eletronicamente por **Admilton Marques da Silva, Assistente**, em 14/10/2024, às 10:58, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0547848** e o código CRC **7D1D0D2C**.

Estudo Técnico Preliminar 92/2024

1. Informações Básicas

Número do processo: 7/2024-68

2. Descrição da necessidade

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para a contratação de solução de antivírus, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

3. Área requisitante

Área Requisitante	Responsável
DEPARTAMENTO DE T.I.	Mauricéia Souza Vilela

4. Necessidades de Negócio

Identificação das necessidades de negócio	
1	Ampliar a disponibilidade dos serviços de tecnologia da informação.
2	Proteção contra malwares que possam comprometer as estações de trabalho.
3	Proteção contra malwares que possam comprometer o uso dos servidores.
4	Filtragem de conteúdos maliciosos.
5	Bloqueio de sites suspeitos.
6	Restrição ao acesso de dispositivos infectados, como pendrives e cartões de memória.
7	Prevenção de fraudes, especialmente nas movimentações financeiras e bancárias.

8	Proteção contra vazamento de informações e perda de dados.
9	Suporte técnico e atualização da base de dados por 36 meses;

Os detalhes das especificações encontram-se no **Anexo I**

5. Necessidades Tecnológicas

Identificação das necessidades tecnológicas	
1	Console de Gerenciamento (Centralizado)
2	Gerenciamento por Grupos (Integração com Microsoft Active Directory – AD)
3	Anti-Malware/Anti-Virus
4	Anti-Ransomware
5	IPS host
6	IDS host
7	Firewall host
8	Filtro de conteúdo Web (Classificação de Site)
9	Suporte a Windows e Linux

10	Proteção para Solução de email (Microsoft Exchange)
11	Proteção para Solução de Diretório (AD)
12	Gerenciamento de vulnerabilidades e correções
13	Integração com soluções de SIEM
14	Controle de Dispositivos (USB)
15	Proteção proativa e instantânea contra ameaças desconhecidas
17	Monitorar o comportamento do aplicativos
18	Interromper atividades potencialmente prejudiciais em tempo real
19	Usar sensores que coletam dados comportamentais de dispositivos endpoint para identificar potenciais ataques
20	Monitora pastas protegidas para evitar gravação não autorizada

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Repasse de informações sobre a solução através de treinamento a ser realizado logo após assinatura do contrato de prestação dos serviços para pelo menos 2 (dois) colaboradores do Departamento de TI do Conselho Regional de Contabilidade de Goiás, de acordo com as especificações técnicas em anexo deste ETP.

7. Estimativa da demanda - quantidade de bens e serviços

Este estudo visa a contratação de solução de antivírus para os estações de de trabalho, notebooks e servidores (máquinas) dos departamentos do Conselho Regional de Contabilidade do Estado de Goiás(CRCGO).

Para identificar a demanda a ser contratada para cada unidade, foi realizado um levantamento de necessidades junto aos respectivos responsáveis.

O registro do quantitativo de itens que compõem a solução consta na tabela abaixo. As quantidades levantadas foram baseadas na utilização atual e necessidade futura.

Unidade Organizacional	Justificativa	Quantidade
CRCGO	Demanda própria	56
SERVIÇO DE IMPLANTAÇÃO /IMPLEMENTAÇÃO	Demanda própria	1
Total		56

8. Levantamento de soluções

3.1 - IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	Descrição da solução (ou cenário)
1	<p>Renovação de licenciamento da solução atual de antivírus</p> <p>Essa alternativa consiste na renovação da última licença de antivírus adquirida pelo Ifes, possibilitando atualização tecnológica de modo a aumentar o nível de segurança e reduzir falhas de segurança e técnicas.</p>
2	<p>Implantar solução de antivírus Gratuita</p> <p>Essa alternativa consiste em implantar uma solução <i>open source</i> ou gratuita para prover o recurso desejado (antivírus) a um custo operacional de implantação da solução.</p>
3	<p>Contratação de Nova Solução de antivírus</p> <p>Essa alternativa consiste na aquisição de uma nova solução de antivírus, possibilitando atualização tecnológica de modo a aumentar a nível de segurança e reduzir falhas de segurança e técnicas.</p>

9. Análise comparativa de soluções

Solução 1 - A última licença de antivírus adquirida pelo CRCGO foi no ano de 2024, sendo que sua vigência foi de 01/11/2021 a 01/11/2024. A solução está

obsoleta porque a licença não atende a nova demanda de filtros de antivírus, e também pela nova quantidade de dispositivos a serem implementados, tal solução, não sendo possível a sua renovação.

Solução 2 - Nessa solução temos um ganho tecnológico considerável, pois é utilizado versões de antivírus mais atuais, com novas tecnologias integradas. Porém o custo operacional é muito grande, das equipes de atendimento, o gerenciamento dessa solução não é centralizado sendo necessário o deslocamento de técnico até estação de trabalho, estando expostos às seguintes questões críticas:

- A. 1. Gerenciamento não centralizado sendo que centralização é um dos requisitos tecnológicos;
- B. 2. Não há Integração com soluções de SIEM
- C. 3. Não há Gerenciamento de vulnerabilidades e correções

Diante do exposto, do ponto de vista da eficiência e da economicidade, a alternativa em questão não atende plenamente às necessidades de negócio elencadas e, portanto, é considerada inviável.

Solução 3 - A aquisição de uma nova licença de antivírus, que atenda aos requisitos de negócio e requisitos tecnológicos estabelecidos neste ETP, possibilitará a atualização de estações de trabalho e servidores (máquinas), aumentando o nível de segurança e, conseqüentemente, reduzindo o número de falhas de segurança.

Além da utilização de uma base de dados de vacinas atualizada rotineiramente, a ferramenta se comunicará com os clientes por meio de um agente instalado, possibilitando o gerenciamento centralizado por meio do software de gerenciamento.

A qualidade do produto, a segurança e o suporte técnico durante o prazo de vigência do contrato, são fatores que tornam essa solução mais atrativa para o serviço público, tendo em vista o grau de confidencialidade das informações.

Além do que, o atual antivírus, de acordo com o Departamento de TI, atende perfeitamente ao perfil do CRCGO, no quesito, segurança. A atual solução de antivírus, é o BIT DEFENDER PREMIUM.

Diante do exposto, esta é a solução considerada viável pela Equipe de Planejamento da Contratação.

Requisito	Solução	Sim	Não	Não se aplica
-----------	---------	-----	-----	---------------

A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	x		
	Solução 2			x
	Solução 3	x		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			x
	Solução 2			x
	Solução 3			x
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			x
	Solução 2	x		
	Solução 3			x
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	x		
	Solução 2	x		
	Solução 3	x		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			x
	Solução 2			x
	Solução 3			x
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			x
	Solução 2			x
	Solução 3			x

10. Registro de soluções consideradas inviáveis

Conforme a análise individual das soluções da seção anterior, as soluções: “Renovação de licenciamento da solução atual de antivírus” e “Implantar solução de antivírus Gratuita” não são consideradas as mais vantajosas no atual cenário da instituição, quando comparada com a solução “Contratação de Nova Solução de antivírus”.

11. Análise comparativa de custos (TCO)

Para realizar análise comparativa de custo, foi realizado uma consulta de preço de soluções de Antivírus no painel de preços, considerando pregões realizados nos últimos 6 meses. a partir dessas informações foi confeccionado a tabela abaixo:

inciso IN 65/2021	Razão Social Do Fornecedor	CNPJ	Valor Da Proposta Final
FORNECEDOR	DSX IT.SOLUTIONS	47.009.544/0001-88	R\$ 280,00
PLATAFORMA DE PESQUISA DE PREÇOS - BANCO DE PREÇO	NP TECNOLOGIA E GESTAO DE DADOS LTDA	07.797.967/0001-95,	R\$ 272,37
MÓDULO DE PESQUISA DE PREÇOS	COMPRAS.GOV	Open Government Partnership - OGP	R\$ 677,20
		Valor Unitário Médio da Licença	R\$ 409,85

A tabela acima foi construída considerando critérios técnicos e quantitativos semelhantes ao cenário exposto no Documento de Formação de Demanda(DFD), pela quantidade de bens e serviços. Foram considerados atendimento aos incisos I e III da Instrução normativa 65 de 2021. Calculamos o preço médio entre as propostas vencedoras resultando no valor presente na tabela. Baseado na Estimativa do DFD - quantidade de bens e serviços temos 56 licenças a serem adquiridas e o serviço de implementação, instalação, reconfiguração e análise, nesse caso, considerando o valor médio obtido da tabela acima e o número de licenças já citado temos tabela abaixo:

item	Descrição do serviço	valor unitário	quantidade	valor total	valor total global
	Cessão de uso de solução				

01	de licença de antivírus, por 3 (três) anos.	R\$ 409,85	56	R\$ 22.951,97	R\$ 22.951,97
02	Serviço de implementação, instalação, reconfiguração e análise.	R\$ 1.500,00	1	R\$ 1.500,00	R\$ 1.500,00
VALOR TOTAL					R\$ 24.451,97

12. Descrição da solução de TIC a ser contratada

Descrição da solução a ser contratada está presente no DFD.

13. Estimativa de custo total da contratação

Valor (R\$): 24.451,97

Para realizar análise comparativa de custo, foi realizado uma consulta de preço de soluções de Antivírus no painel de preços, com fornecedores e com plataforma de pesquisa de preços. a partir dessas informações foi confeccionado a tabela abaixo:

Item	Descrição do serviço	valor unitário	quantidade	valor total	valor total global
01	Cessão de uso de solução de licença de antivírus, por 3(três) anos.	R\$ 409,85	56	R\$ 22.951,97	R\$ 22.951,97
02	Serviço de implementação, instalação, reconfiguração e análise.	R\$ 1.500,00	1	R\$ 1.500,00	R\$ 1.500,00
VALOR TOTAL					R\$ 24.451,97

A tabela acima foi construída considerando critérios técnicos e quantitativos semelhantes ao cenário exposto no Anexo I - Especificações Técnicas e na Estimativa da demanda - foi realizado uma consulta de preço de soluções de Antivírus no painel de preços, com fornecedores e com plataforma de pesquisa de preços Calculamos o preço médio entre as propostas vencedoras resultando no valor presente na tabela. Baseado na Estimativa da demanda - quantidade de bens e serviços temos 56 licenças totalizando R\$ 24.451,97(vinte e quatro mil quatrocentos e cinquenta e um reais e noventa e sete centavos)

14. Justificativa técnica da escolha da solução

A aquisição de uma nova licença de antivírus, que atenda aos requisitos de negócio e requisitos tecnológicos estabelecidos neste ETP, possibilitará a atualização de estações de trabalho e servidores (máquinas), aumentando o nível de segurança e, conseqüentemente, reduzindo o número de falhas de segurança.

Além da utilização de uma base de dados de vacinas atualizada rotineiramente, a ferramenta se comunicará com os clientes por meio de um agente instalado, possibilitando o gerenciamento centralizado por meio do software de gerenciamento.

A qualidade do produto, a segurança e o suporte técnico durante o prazo de vigência do contrato, são fatores que tornam essa solução mais atrativa para o serviço público, tendo em vista o grau de confidencialidade das informações.

Diante do exposto, esta é a solução considerada viável pela Equipe de Planejamento da Contratação.

15. Justificativa econômica da escolha da solução

Considerando que a falta da solução em questão permitirá a ocorrência de eventos catastróficos com impactos negativos incalculáveis para o CRCGO, sua contratação já se caracteriza justificável do ponto de vista econômico já que trará redução de custos imprevistos com mitigação de riscos. Outro fato é que a solução pretendida já está devidamente consagrada como melhor alternativa de mercado para as demandas existentes, justificando-se economicamente também pela grande quantidade de fornecedores que poderão participar do certame com perspectiva de redução dos valores de referência e conseqüente economia para a administração.

16. Benefícios a serem alcançados com a contratação

Manutenção dos níveis de segurança da informação desejáveis para as atividades orgânicas do CRCGO, de forma ininterrupta e dentro do que preconizam as boas práticas de mercado.

17. Providências a serem Adotadas

Estratégia de autonomia, eficiência e total domínio do uso da solução pelo CRCGO

O Departamento de TI, poderá adotar a forma de repasse de conhecimento entre os integrantes da equipe que gerenciará a solução contratada. O repasse de conhecimento se dará na forma de capacitação ou treinamento na solução e seus recursos. A referida atividade de treinamento deverá ser capaz de dotar aos

participantes a capacidade de instalar, operar e manter todos os módulos e recursos da solução fornecida pela contratada. Serão capacitados 2 (dois) integrantes da equipe responsável pelo gerenciamento da solução contratada. Juntamente com o repasse de conhecimento, O Departamento de TI, deverá realizar o armazenamento da documentação dos produtos contratados em ambiente digital.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Considerando as análises apresentadas nas soluções 1, 2 e 3, e com base nos requisitos técnicos e de negócio estabelecidos no ETP, declara-se a viabilidade da Solução 3 para a aquisição de uma nova licença de antivírus para o CRCGO.

Justificativa:

A Solução 3 apresenta os seguintes benefícios que a tornam a opção mais adequada para atender às necessidades do CRCGO:

- **Alinhamento com os requisitos técnicos e de negócio:** A nova licença de antivírus atenderá plenamente aos requisitos estabelecidos no ETP, garantindo a atualização das estações de trabalho e servidores, aumentando o nível de segurança e reduzindo o número de falhas de segurança.
- **Gerenciamento centralizado:** A ferramenta de antivírus possibilitará o gerenciamento centralizado de todas as máquinas, o que otimiza o trabalho da equipe de TI e garante maior controle sobre a segurança da rede.
- **Base de dados de vacinas atualizada:** A atualização constante da base de dados de vacinas assegura a proteção contra as mais recentes ameaças cibernéticas.
- **Comunicação com os clientes por meio de um agente instalado:** O agente instalado nas máquinas permite um monitoramento mais eficiente e a detecção de possíveis vulnerabilidades.
- **Qualidade do produto, segurança e suporte técnico:** A solução escolhida oferece um alto nível de segurança e confiabilidade, além de contar com um suporte técnico especializado durante todo o período de vigência do contrato.
- **Adequação ao perfil do CRCGO:** Conforme avaliação do Departamento de TI, o antivírus BIT DEFENDER PREMIUM atende perfeitamente ao perfil de segurança do CRCGO.

Em contrapartida, as demais soluções apresentam as seguintes limitações:

- **Solução 1:** A licença atual está obsoleta e não atende às novas demandas, além de não ser possível a sua renovação.
- **Solução 2:** Apresenta um alto custo operacional e não atende aos requisitos de centralização e integração com outras soluções de segurança.

Conclusão:


Diante dos fatos apresentados, a Solução 3 é a que melhor se adequa aos requisitos técnicos e de negócio do CRCGO, garantindo um alto nível de segurança da informação e otimizando a gestão da segurança da rede.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).


ADMILTON MARQUES DA SILVA

Equipe de apoio

 Assinou eletronicamente em 07/10/2024 às 16:37:55.

MAURICEIA DE SOUSA VILELA

Demandante

 Assinou eletronicamente em 08/10/2024 às 09:03:27.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - SEI_0536980_Protocolo_de_procedimentos_especificos.pdf (90.34 KB)

**Anexo I -
SEI_0536980_Protocolo_de_procedimentos_especificos.pdf**



CONSELHO REGIONAL DE CONTABILIDADE DE GOIÁS
Rua 107 n.º 151, - Bairro Setor Sul, Goiânia/GO, CEP 74085-060
Telefone: (62) 3240-2211/2200 - <https://crcgo.org.br/novo/> E-mail: crcgo@crcgo.org

Especificações restritas para contratação da solução:

CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE LICENÇAS DE SOFTWARE DE ANTIVÍRUS SUPORTE PELO PERÍODO DE 3 ANOS

1. Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.
 - 1.1. Possuir console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;
 - 1.2. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;
 - 1.3. O produto deverá possuir no mínimo os seguintes módulos:
 - 1.4. Console de Gerenciamento fornecendo funcionalidades de gestão;
 - 1.5. Módulos para estações físicas, laptops e servidores;
 - 1.6. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;
 - 1.7. Utilizar o conceito de heurística;
 - 1.8. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
 - 1.9. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;
 - 1.10. Oferecer inventário de softwares;
 - 1.11. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;
 - 1.12. Oferecer proteção por base de assinaturas;

2. Console De Gerenciamento

- 2.1. Instalação e configuração
- 2.2. Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).
- 2.3. Deverá suportar no mínimos os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-in-a-Box;
- 2.4. Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;
- 2.5. Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;
- 2.6. Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;
- 2.7. O mecanismo de varredura deverá estar disponível para download separadamente;
- 2.8. A solução deverá permitir a inclusão de um modulo de balanceamento para casos em vários servidores tenham a

mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);
2.9.Deve ser totalmente em português.

3. Características Gerais

- 3.1.Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;
- 3.2.Permitir que o administrador escolha qual o pacote será atualizado;
- 3.3.As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;
- 3.4.No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,
- 3.5.Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;
- 3.6.Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;
- 3.7.Inventário da Rede
- 3.8.Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;
- 3.9.Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
- 3.10.Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
- 3.11.Descoberta de rede para máquinas em grupo de trabalho;
- 3.12.Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;
- 3.13.Possibilitar a instalação remota e desinstalação remota do antivírus;
- 3.14.Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- 3.15.Possuir tarefas remotas e configuráveis de Scan;
- 3.16.Possuir tarefa de reinicialização remota de estação ou servidor;
- 3.17.Assinar políticas para no mínimo os níveis: Computador, Máquina Virtual ou Possuir a propriedade detalhada de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política Assinada, ultimo status de malware;

4. Políticas

- 4.1.Modelo único para todos os equipamentos, seja físico ou virtual;
- 4.2.Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;
- 4.3.Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

5. Relatórios

- 5.1.Relatório para cada serviço de segurança;
- 5.2.Facilidade de usar e visualização simplificada;
- 5.3.Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;
- 5.4.Filtros de agendamento de relatórios;
- 5.5.Arquivo com todas as instâncias de relatório agendados;
- 5.6.Exportar o relatório nos formatos .pdf e/ou .csv;
- 5.7.Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.

6. Quarentena

- 6.1.Restauração remota, com configuração de localidade e deleção;
- 6.2.Criação e exclusão para arquivos restaurados;

7. Usuários

- 7.1.Administração baseada em regras;
- 7.2.Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da solução, Administrador de rede - Gerente dos serviços de segurança;

- 7.3. Relatório - Monitora e cria relatórios;
- 7.4. Deverá ser possível customizar um tipo de usuário;
- 7.5. Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;
- 7.6. Logs de utilização;
- 7.7. Registrar as ações do usuário na console de gerenciamento;
- 7.8. Detalhar cada ação do usuário;
- 7.9. Permitir busca complexa baseada em ações do usuário, intervalos de tempo;

8. Certificado de Segurança

- 8.1. Deverá prover o acesso via HTTPS;
- 8.2. Deverá permitir a importação de certificados digitais;
- 8.3. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais;

9. Proteção Para Estações De Trabalho E Servidores Físicos

- 9.1. Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Híbrido, Scan Central;
- 9.2. Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso a internet; Instalar o antivírus sem o módulo de firewall;
- 9.3. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e 64Bits, Windows 7 32 e 64Bits.
- 9.4. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2022, Windows Server 2019 Core, Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2.
- 9.5. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

10. Gerenciamento e Instalação Remota

- 10.1. Deverá permitir ao administrador customizar a instalação;
- 10.2. A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerencia web;
- 10.3. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;
- 10.4. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;
- 10.5. Através da console, o administrador poderá enviar uma política única para configurar o antivírus;
- 10.6. A console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits, deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
- 10.7. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado;

11. Proteção Para Estações e Servidores Virtuais

- 11.1. Proteção de antivírus dedicado para ambientes virtuais;
- 11.2. Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;
- 11.3. A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;
- 11.4. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;
- 11.5. O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;

12. Funções Gerais

12.1. Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;

12.2. Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;

13. Requisitos Mínimos suportados pelo Sistema.

13.1. Plataformas de Virtualização: VMware vSphere and vCenter Server:

versão 6.5;

version 6.7, incluindo update 1, update 2a e update 3;

version 7.0, incluindo update 1, update 2, update 2b, update 2c e update 2d;

version 8.0, incluindo update 1, update 2.

VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x

VMware Workstation 11.x, 10.x, 9.x, 8.0.6

VMware Player 7.x, 6.x, 5.x

Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2.

Citrix Virtual Apps e Desktops 7 1808, 7 1811, 7 1903, 7 1906

Citrix XenApp e XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR

Citrix VDI-in-a-Box 5.x

Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (incluindo Hyper-V Hypervisor)

Red Hat Enterprise Virtualization 3.0 (incluindo KVM Hypervisor)

Oracle VM 3.0

Oracle VM VirtualBox 5.2, 5.1

Nutanix Prism com AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)

Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 e 20190916.294 (Community Edition)

13.2. Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10

13.3. Sistemas Operacionais Servidores: Windows Server 2022 Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2, Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

14. Componentes e Funcionalidade do Antivírus Geral

14.1. Deverá fazer scan em tempo real automático;

14.2. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;

14.3. Escaneamento de comportamento heurístico;

14.4. Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como: CD/DVD, Discos Externos, Pen-Drivers, Deverá permitir a escolha e configuração de pastas a serem escaneada;

- 14.5. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;
- 14.6. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;
- 14.7. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho;
- 14.8. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;
- 14.9. O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;
- 14.10. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
- 14.11. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
- 14.12. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
- 14.13. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
- 14.14. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

15. Controle de Usuário

- 15.1. Deverá ter módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso a internet, Bloqueio de acesso a aplicações definidas pelo administrador;

16. Controle do Dispositivo

- 16.1. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
- 16.2. Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDROM/DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;
- 16.3. Deverá permitir regras de definição de bloqueio/desbloqueio;
- 16.4. Deverá permitir regras de exclusão;

17. Atualização

- 17.1. Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;
- 17.2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
- 17.3. Permitir atualizações de assinatura de hora em hora;
- 17.4. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

18. Proteção para caixa de e-mail:

- 18.1. Fornecer proteção para ambiente Exchange
- 18.2. Oferecer tecnologia para proteção contra spam;
- 18.3. Oferecer análise comportamental e proteção para zero-day;
- 18.4. Oferecer proteção contra vírus e tentativas de phishing;

19. Criptografia

- 19.1. Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivirus.
- 19.2. Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);
- 19.3. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
- 19.4. Deverá ser compatível com:

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

20. Proteção Avançada NGAV

20.1. Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.

20.2. Detectar e parar, bloquear e interromper malwares sem arquivos.

20.3. Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.

20.4. Reparo e resposta automatizada a ameaças

20.5. Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal intencionadas. Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.

20.6. Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.

20.7. Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.

20.8. Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web. Deverá permitir que os administradores de segurança ajustem a proteção para combater os riscos.

21. Machine Learning

21.1. As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.

21.2. A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinar continuamente com bilhões de amostras de arquivos legítimos e maliciosos devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.

21.3. Detecção e Resposta - EDR

21.4. Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades de XEDR para detectar ataques avançados em vários terminais em infraestruturas híbridas (estações de trabalho ou servidores executando vários sistemas operativos)

21.5. Deverá analisar continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identificar ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de USBs comprometidos, infecções recorrentes, etc

22. Sandbox

22.1. Sandbox integrado nos terminais que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas.

23. Antiexploit Avançado

23.1. Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja: Flash ou Java). Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (return-oriented programming), etc.

24. Inspetor de processo

24.1. O Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (seqüestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem etc. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.



Documento assinado eletronicamente por **Mauricéia de Sousa Vilela, Coordenadora**, em 07/10/2024, às 16:22, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0536980** e o código CRC **45511B4F**.

CONSELHO REGIONAL DE CONTABILIDADE DE GOIÁS

MAPA DE COMPARATIVO DE PREÇOS

ITEM	DESCRIÇÃO DO OBJETO	PAINEL DE PREÇOS		PESQUISA COM FORNECEDOR	VALOR MÉDIO * 56 LICENÇAS	
		NP TECNOLOGIA E GESTAO DE DADOS LTDA 07.797.967/0001-95	COMPRAS.GOV OPEN GOVERNMENT PARTNERSHIP-OGP	DSX IT.SOLUTIONS 47.009.544/0001-88		
1	Cessão de uso de solução de 56 licenças de antivírus. por 3 (três) anos.	R\$ 272,37	677,20	R\$ 280,00	R\$ 409,85	R\$ 22,95
2	Serviço de implementação, instalação, reconfiguração e análise.	R\$ 1.500,00			R\$ 1.500,00	R\$ 1,50
VALOR TOTAL GLOBAL						R\$ 24,45

Pesquisa de Preços realizada com base no inciso I e III do art. 5º da Instrução Normativa nº 65 de 7 de julho de 2021, da Secretaria de Gestão do Ministério da Economia.

Foram consultados valores de aquisição em sites especializados e com fornecedores na entrega da demanda.

O critério adotado será o de menor preço, pois se trata de dispensa de licitação, na sua forma eletrônica.

Justificativa anexa a este mapa.

Declaro que no Projeto nº 5010 – Modernização do Parque de Informática (Hardware e Software) está revisto o suporte orçamentário para execução da despesa.

Em 09 de outubro de 2024
Elaborado por

Admilton Marques da Silva
Agente de Contratação



Documento assinado eletronicamente por **Admilton Marques da Silva, Assistente**, em 09/10/2024, às 17:50, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0543032** e o código CRC **201D8414**.

Termo de Referência 95/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
95/2024	926864-CONSELHO REGIONAL DE CONTABILIDADE - GO	ADMILTON MARQUES DA SILVA	09/10/2024 17:21 (v 5.1)
Status	PUBLICADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		000007/2024-68

1. Condições gerais da contratação

TERMO DE REFERÊNCIA

Lei nº 14.133, de 1º de abril de 2021

SERVIÇOS DE TIC

CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE GOIAS

Processo Administrativo nº 9079602110000085.000007/2024-68

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1.1. Contratação de empresa especializada em cessão de uso de licença de antivírus corporativo, por 3(Três) anos, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Cessão de uso de solução de licença de antivírus, por 3(três) anos.	24333	UND	56	R\$ 409,85	R\$ 22.951,97
2	Serviço de Implementação,	30001	SERV	1	R\$ 1.500,00	R\$ 1.500,00

instalação, reconfiguração e análise.					
VALOR TOTAL GLOBAL					R\$ 24.451,97

1.

1.2. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. Fundamentação e descrição da necessidade

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme consta das informações básicas deste termo de referência.

3. Descrição da solução como um todo

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

4. Requisitos da contratação

4. REQUISITOS DA CONTRATAÇÃO

1. Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.

1.1. Possuir console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall,

Deteção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;

1.2. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;

1.3. O produto deverá possuir no mínimo os seguintes módulos:

1.4. Console de Gerenciamento fornecendo funcionalidades de gestão;

1.5. Módulos para estações físicas, laptops e servidores;

1.6. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

1.7. Utilizar o conceito de heurística;

1.8. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);

- 1.9.Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;
- 1.10.Oferecer inventário de softwares;
- 1.11.Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;
- 1.12.Oferecer proteção por base de assinaturas;
2. Console De Gerenciamento
- 2.1.Instalação e configuração
- 2.2.Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).
- 2.3.Deverá suportar no mínimos os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; Xen Desktop, VDI-ina-Box;
- 2.4.Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;
- 2.5.Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;
- 2.6.Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;
- 2.7.O mecanismo de varredura deverá estar disponível para download separadamente;
- 2.8.A solução deverá permitir a inclusão de um modulo de balanceamento para casos em vários servidores tenham a Protocolo de procedimentos específicos na mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);
- 2.9.Deve ser totalmente em português.
3. Características Gerais
- 3.1.Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;
- 3.2.Permitir que o administrador escolha qual o pacote será atualizado;
- 3.3.As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;
- 3.4.No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,
- 3.5.Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;
- 3.6.Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;
- 3.7.Inventário da Rede
- 3.8.Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;
- 3.9.Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
- 3.10.Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
- 3.11.Descoberta de rede para máquinas em grupo de trabalho;
- 3.12.Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;
- 3.13.Possibilitar a instalação remota e desinstalação remota do antivírus;
- 3.14.Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- 3.15.Possuir tarefas remotas e configuráveis de Scan;
- 3.16.Possuir tarefa de reinicialização remota de estação ou servidor;
- 3.17.Assinar políticas para no mínimo os níveis: Computador, Máquina Virtual ou Possuir a propriedade detalhada de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política Assinada, ultimo status de malware;
4. Políticas
- 4.1.Modelo único para todos os equipamentos, seja físico ou virtual;
- 4.2.Cada serviço de segurança deve ter seu modelo configurável de política com opções

específicas de
ativar/desativar;

4.3. Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção

de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

5. Relatórios

5.1. Relatório para cada serviço de segurança;

5.2. Facilidade de usar e visualização simplificada;

5.3. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;

5.4. Filtros de agendamento de relatórios;

5.5. Arquivo com todas as instâncias de relatório agendados;

5.6. Exportar o relatório nos formatos .pdf e/ou .csv;

5.7. Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.

6. Quarentena

6.1. Restauração remota, com configuração de localidade e deleção;

6.2. Criação e exclusão para arquivos restaurados;

7. Usuários

7.1. Administração baseada em regras;

7.2. Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da solução, Administrador de rede - Gerente dos serviços de segurança; Protocolo de procedimentos específicos.

7.3. Relatório - Monitora e cria relatórios;

7.4. Deverá ser possível customizar um tipo de usuário;

7.5. Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;

7.6. Logs de utilização;

7.7. Registrar as ações do usuário na console de gerenciamento;

7.8. Detalhar cada ação do usuário;

7.9. Permitir busca complexa baseada em ações do usuário, intervalos de tempo;

8. Certificado de Segurança

8.1. Deverá prover o acesso via HTTPS;

8.2. Deverá permitir a importação de certificados digitais;

8.3. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais;

9. Proteção Para Estações De Trabalho E Servidores Físicos

9.1. Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Híbrido, Scan Central;

9.2. Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso a internet; Instalar o antivírus sem o módulo de firewall;

9.3. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e 64Bits, Windows 7 32 e 64Bits.

9.4. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2022 Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2.

9.5. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: Ubuntu 14.04

LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server

- 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;
10. Gerenciamento e Instalação Remota
- 10.1. Deverá permitir ao administrador customizar a instalação;
- 10.2. A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerencia web;
- 10.3. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;
- 10.4. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;
- 10.5. Através da console, o administrador poderá enviar uma política única para configurar o antivírus;
- 10.6. A console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits, deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
- 10.7. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado;
11. Proteção Para Estações e Servidores Virtuais
- 11.1. Proteção de antivírus dedicado para ambientes virtuais;
- 11.2. Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;
- 11.3. A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;
- 11.4. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;
- 11.5. O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;
12. Funções Gerais
- 12.1. Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;
- 12.2. Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;
13. Requisitos Mínimos suportados pelo Sistema.
- 13.1. Plataformas de Virtualização: VMware vSphere and vCenter Server: versão 6.5; version 6.7, incluindo update 1, update 2a e update 3; version 7.0, incluindo update 1, update 2, update 2b, update 2c e update 2d; version 8.0, incluindo update 1, update 2. VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x VMware Workstation 11.x, 10.x, 9.x, 8.0.6 VMware Player 7.x, 6.x, 5.x Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2. Citrix Virtual Apps e Desktops 7 1808, 7 1811, 7 1903, 7 1906 Citrix XenApp e XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR Citrix VDI-in-a-Box 5.x Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (incluindo Hyper-V Hypervisor) Red Hat Enterprise Virtualization 3.0 (incluindo KVM Hypervisor) Oracle VM 3.0 Oracle VM VirtualBox 5.2, 5.1 Nutanix Prism com AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)

- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 e 20190916.294 (Community Edition) 13.2.Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10
- 13.3.Sistemas Operacionais Servidores: Windows Server 2022 Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2, Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;
14. Componentes e Funcionalidade do Antivírus Geral
- 14.1.Deverá fazer scan em tempo real automático;
- 14.2.Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;
- 14.3.Escaneamento de comportamento heurístico;
- 14.4.Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como: CD/DVD, Discos Externos, Pen-Drivers, Deverá permitir a escolha e configuração de pastas a serem escaneadas;
- 14.5.Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;
- 14.6.Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;
- 14.7.O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho;
- 14.8.Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;
- 14.9.O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;
- 14.10.Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
- 14.11.Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
- 14.12.Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
- 14.13.Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
- 14.14.Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;
15. Controle de Usuário
- 15.1.Deverá ter módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso a internet, Bloqueio de acesso a aplicações definidas pelo administrador;
16. Controle do Dispositivo
- 16.1.Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
- 16.2.Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDROM /DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;
- 16.3.Deverá permitir regras de definição de bloqueio/desbloqueio;
- 16.4.Deverá permitir regras de exclusão;
17. Atualização
- 17.1.Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;
- 17.2.Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
- 17.3.Permitir atualizações de assinatura de hora em hora;

17.4. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

18. Proteção para caixa de e-mail:

18.1. Fornecer proteção para ambiente Exchange

18.2. Oferecer tecnologia para proteção contra spam;

18.3. Oferecer análise comportamental e proteção para zero-day;

18.4. Oferecer proteção contra vírus e tentativas de phishing;

19. Criptografia

19.1. Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-

premise com módulo de Criptografia presente na mesma Console do Antivirus.

19.2. Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);

19.3. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;

19.4. Deverá ser compatível com:

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

20. Proteção Avançada NGAV

20.1. Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como

eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.

20.2. Detectar e parar, bloquear e interromper malwares sem arquivos.

20.3. Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.

20.4. Reparo e resposta automatizada a ameaças

20.5. Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal intencionadas. Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.

20.6. Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.

20.7. Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.

20.8. Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de

máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web. Deverá permitir que os administradores de segurança ajustem a proteção para combater os riscos.

21. Machine Learning

21.1. As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para

prever e bloquear os ataques avançados.

21.2.A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinarem continuamente com bilhões de amostras de arquivos legítimos e maliciosas devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.

21.3.Detecção e Resposta - EDR

21.4.Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades de XEDR para detectar ataques avançados em vários terminais em

infraestruturas híbridas (estações de trabalho ou servidores executando vários sistemas operativos)

21.5. Deverá analisar continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identificar ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de USBs comprometidos, infecções recorrentes, etc

22. Sandbox

22.1.Sandbox integrado nos terminais que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas.

23. Antiexploit Avançado

23.1.Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja:Flash ou Java). Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (returnoriented programming), etc.

24. Inspetor de processo

24.1.O Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente

todos os processos em execução no sistema operacional. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (seqüestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem etc. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar demalwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

5. Modelo de execução do objeto

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Condições de Execução e Garantia

5.1.1. A CONTRATADA se obriga, no período mínimo de 12 (doze) meses, contados a partir da entrega das licenças em nome da CONTRATANTE, disponibilizar e os serviços de garantir autenticação em nuvem por e-mail para os usuários das licenças, INCLUINDO todos os pacotes de atualização, que porventura surjam para as versões ofertadas.

5.1.2. à Contratante o pleno acesso ao site do fabricante do software, com direito a garantir consultas a quaisquer bases de dados disponíveis para usuários;

5.1.3. Não deverá haver qualquer limitação para o suporte técnico;

5.1.4. Na entrega do produto licenciado, por meio eletrônico, deverá ser enviado para o endereço eletrônico: informatica@crcgo.org.br, em nome da demandante, Mauricéia Souza Vilela

5.1.5. O ateste do recebimento das licenças, será emitido pelo servidor apontado no subitem 5.1.4. e, deverá ocorrer no prazo máximo de cinco dias úteis, contados a partir do primeiro dia útil subsequente ao da entrega.

5.2. Horário da prestação dos serviços

5.2.1. Os serviços serão prestados de forma online com suporte liberado em horário comercial de 09h00 a às 18h00 de segunda a sexta feira, durante o expediente do CRCGO.

6. Modelo de gestão do contrato

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterà informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

1. 6.9. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

1.

6.10. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

6.11. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II);

6.12. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

6.13. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

6.14. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

6.15. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

Fiscalização Administrativa

1.

6.16. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

6.17. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

1.

6.18. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das

alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

6.19. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

6.20. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

6.21. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

6.23. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.24. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.25. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. Critérios de medição e pagamento

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. O pagamento do objeto a ser adquirido será realizado em até 10 (dez) dias úteis, após a atestação do recebimento.

7.2. A CONTRATADA deverá emitir a respectiva nota fiscal/fatura devidamente discriminada, em nome do Contratante.

7.3. Qualquer atraso ocorrido na apresentação da fatura ou da nota fiscal, ou documentos exigidos como condição para pagamento por parte da CONTRATADA, importará na prorrogação automática do prazo de vencimento da obrigação do Contratante.

7.4. O pagamento será realizado por meio de ordem bancária, para crédito na instituição financeira, agência e conta corrente indicados pelo contratado.

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

8. Forma e critérios de seleção e regime

8. FORMA E CRITÉRIOS DE SELEÇÃO E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

1.

8.1. O contratado será selecionado por meio da realização de procedimento de dispensa de licitação, na forma eletrônica, com fundamento na hipótese do art. 75, inciso II da Lei nº 14.133/2021, que culminará com a seleção da proposta de MENOR PREÇO POR ITEM.

Exigências de habilitação

1.

8.2. *Previamente à celebração do contrato, a Administração verificará o eventual descumprimento das condições para contratação, especialmente quanto à existência de sanção que a impeça, mediante a consulta a cadastros informativos oficiais, tais como:*

a) SICAF;

b) *Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);*

c) *Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>)*

1.

8.3. *A consulta aos cadastros será realizada em nome da empresa interessada e de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.*

8.4. *Caso conste na Consulta de Situação do interessado a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.*

8.5. *A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.*

8.6. *O interessado será convocado para manifestação previamente a uma eventual negativa de contratação.*

8.7. *Caso atendidas as condições para contratação, a habilitação do interessado será verificada por meio do SICAF, nos documentos por ele abrangidos.*

8.8. *É dever do interessado manter atualizada a respectiva documentação constante do SICAF, ou encaminhar, quando solicitado pela Administração, a respectiva documentação atualizada.*

8.9. *Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.*

8.10. *Se o interessado for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.*

8.11. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

8.12. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos, que serão exigidos conforme sua natureza jurídica:

Habilitação jurídica

1.

8.13. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.14. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.15. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor/>;

8.16. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.17. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

8.18. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.19. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

8.20. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

8.21. Ato de autorização para o exercício da atividade de (especificar a atividade contratada sujeita à autorização), expedido por (especificar o órgão competente) nos termos do art. da (Lei/Decreto) n°

8.22. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

1.

8.23. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.24. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.25. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.26. declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;

8.27. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.28. Prova de inscrição no cadastro de contribuintes [Estadual/Distrital] ou [Municipal/Distrital] relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.29. Prova de regularidade com a Fazenda [Estadual/Distrital] ou [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.30. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] ou [Municipal/Distrital] relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.31. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

1.

8.32. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua contratação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

8.33. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

8.34. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

8.34.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

8.34.2. As empresas criadas no exercício financeiro da contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e

8.34.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

8.34.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

8.35. *Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC). O SICAF Poderá substituir nesse quesito.*

8.36. *As empresas criadas no exercício financeiro da contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).*

8.37. *O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pela empresa.*

Qualificação Técnica

1.

8.38. *Declaração de que o interessado tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação;*

8.39. *A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do interessado acerca do conhecimento pleno das condições e peculiaridades da contratação.*

8.40. *Registro ou inscrição da empresa na entidade profissional competente(escrever por extenso, se o caso), em plena validade;*

8.40.1. *Sociedades empresárias estrangeiras atenderão à exigência por meio da apresentação, no momento da assinatura do contrato, da solicitação de registro perante a entidade profissional competente no Brasil.*

8.41. *Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.*

8.41.1. *Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.*

8.41.2. *Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial da empresa interessada.*

8.41.3. *O interessado disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.*

8.42. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

8.42.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

8.42.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.42.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

8.42.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

8.42.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

8.43.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da contratação direta; e

8.44.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

9. Estimativas do valor da contratação

Valor (R\$): 24.451,97

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. Para realizar análise comparativa de custo, foi realizado uma consulta de preço de soluções de Antivírus no painel de preços, com fornecedores e com plataforma de pesquisa de preços. a partir dessas informações foi confeccionado a tabela abaixo:

Item	Descrição do serviço	Valor unitário	quantidade	Valor total	Valor Global
01	Cessão de uso de solução de licença de antivírus, por 3 (três) anos.	409,85	56	22.951,97	22.951,97
02	Serviço de implementação, instalação, reconfiguração e análise.	1.500,00	1	1.500,00	1.500,00
Valor total					24.451,97

9.2 MODELO DE PROPOSTA

A empresa classificada em primeiro lugar, deverá formalizar sua proposta, e ajustar seus valores conforme o modelo de proposta abaixo:

DISPENSA ELETRONICA Nº 90049/2024
 PROCESSO ADMINISTRATIVO SEI 9079602110000085.000007/2024-68
 TIPO: Menor Preço por item

OBJETO: A presente dispensa de licitação, na sua forma eletrônica, visa a contratação de empresa para cessão de uso de 56 licença corporativas de antivírus e sua implementação, instalação, reconfiguração e análise para o CRCGO.

A (empresa)..... inscrita no CNPJ sob nº.
, estabelecida
 na....., nº....., telefone/fax
 nº....., e-mail....., propõe fornecer o objeto
 licitado, nos seguintes preços e condições:

Aquisição de licenças antivírus:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
01					
02					
VALOR TOTAL					

O prazo de validade de nossa proposta é de 120 dias corridos, a contar da data da apresentação da (proposta).

II – Prazo de Pagamento: Conforme Edital.

III – Declaramos que o VALOR TOTAL DA PROPOSTA é irrevogável, e estão incluídos:

- a) os tributos, fretes, alimentação, estadia, encargos sociais;
- b) as despesas e obrigações financeiras de qualquer natureza; e,
- c) todos os componentes de custo dos bens necessários à perfeita satisfação do objeto desta Dispensa de licitação.

IV – Declaramos, que possuímos condições de atender os serviços estabelecidos no prazo assinalado, de que o(s) preço(s) cotado(s) inclui(em) todos os custos e despesas necessárias ao cumprimento integral das obrigações decorrentes desta dispensa de licitação, de que os e cotados atendem integralmente às especificações descritas no Anexo - I deste termo de referência, bem como seu compromisso de prestar os serviços que lhe for(em) julgados(s).

V– Declaramos, ainda, conhecer integralmente os termos do aviso de contratação nº 49/2024 e seus anexos, aos quais nos sujeitamos.

DADOS DO RESPONSÁVEL PELA ASSINATURA DO CONTRATO

ME:

F: RG:

ENDEREÇO COMERCIAL:

ENDEREÇO RESIDENCIAL:

FONE:

EMAIL:

DADOS BANCÁRIOS

BANCO NÚMERO DO BANCO:

AGÊNCIA: CONTA CORRENTE:

Local, xx de xxxx de 2024.

Ass. Responsável / Repres. Legal

Cargo:

CPF:

Carimbo da Empresa

NOTA: O proponente deverá rubricar a 1ª via desta planilha/proposta.

(papel timbrado da licitante)

ADEQUAÇÃO ORÇAMENTÁRIA

1.

9.2. As despesas decorrentes da presente contratação correrão à conta de recursos próprios, conforme PAC 2024.

10. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

ADMILTON MARQUES DA SILVA

Equipe de apoio



Assinou eletronicamente em 09/10/2024 às 17:18:10.

MAURICEIA DE SOUSA VILELA

Demandante



Assinou eletronicamente em 09/10/2024 às 17:18:29.

AVISO DE CONTRATAÇÃO DIRETA

Aviso de

DISPENSA ELETRÔNICA

90049/2024

CONTRATANTE (UASG)

CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE GOIAS (926864)

OBJETO

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA AQUISIÇÃO DE DIREITO DE CESSÃO DE USO DE LICENÇA DE SOLUÇÃO DE ANTIVIRUS PARA 56 DISPOSITIVOS PARA 36(TRINTA E SEIS) MESES, ALÉM DA SUA IMPLEMENTAÇÃO, IMPLANTAÇÃO, INSTALAÇÃO, RECONFIGURAÇÃO E ANÁLISE.

VALOR TOTAL DA CONTRATAÇÃO

R\$ 24.451,97(VINTE E QUATRO MIL QUATROCENTOS E CINQUENTA E UM REAIS E NOVENTA E SETE CENTAVOS)

PERÍODO DE PROPOSTAS

De 15/10/2024 às 08h00m

Até 18/10/2024 às 07h59min

PERÍODO DE LANCES

De 18/10/2024 às 08:05hs

Até 18/10/2024 às 14:05hs

PREFERÊNCIA ME/EPP/EQUIPARADAS

SIM

Sumário

- [1. OBJETO DA CONTRATAÇÃO DIRETA](#)
- [2. PARTICIPAÇÃO NA DISPENSA ELETRÔNICA.](#)
- [3. INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL](#)
- [4. FASE DE LANCES](#)
- [5. JULGAMENTO DAS PROPOSTAS DE PREÇO](#)
- [6. HABILITAÇÃO](#)
- [7. CONTRATAÇÃO](#)

[8. SANÇÕES](#)

[9. DAS DISPOSIÇÕES GERAIS](#)

CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE GOIÁS

AVISO DE DISPENSA ELETRÔNICA Nº 90049/2024 9079602110000085.000007/2024-68

Torna-se público que o Conselho Regional de Contabilidade do Estado de Goiás por meio do Departamento de Licitações e Compras realizará Dispensa Eletrônica, com critério de julgamento Menor Preço por item, na hipótese do art. 75, *Inciso II* nos termos da LEI Nº 14.133, DE 1º DE ABRIL DE 2021, da INSTRUÇÃO NORMATIVA SEGES/ME nº 67/2021, Lei LEI COMPLEMENTAR Nº 123, DE 14 DE DEZEMBRO DE 2006 e demais legislações aplicáveis.

Data da sessão: 18/10/2024

Link: <https://www.gov.br/compras/pt-br>

Horário da Fase de Lances: 08:05hs da manhã

1. OBJETO DA CONTRATAÇÃO DIRETA

1.1. O objeto da presente dispensa é a escolha da proposta mais vantajosa para a Contratação de Empresa Especializada para Aquisição de Direito de Cessão de Uso de Licença de Solução de Antivírus para 56 Dispositivos para 36(trinta e Seis) Meses, Além da sua Implementação, Implantação, Instalação, Reconfiguração e Análise, conforme condições, quantidades e exigências estabelecidas neste Aviso de Contratação Direta e seus anexos.

1.2. *A contratação será dividida em item, conforme tabela constante abaixo:*

Itens	Serviço	Quantidade	Valor unitário	Valor global
1.	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA AQUISIÇÃO DE DIREITO DE CESSÃO DE USO DE LICENÇA DE SOLUÇÃO DE ANTIVIRUS PARA 56(CINQUENTA E SEIS) DISPOSITIVOS PARA 36(TRINTA E SEIS) MESES, ALÉM DA SUA IMPLEMENTAÇÃO, IMPLANTAÇÃO, INSTALAÇÃO, RECONFIGURAÇÃO E ANÁLISE.	01	R\$ 24.451,97	R\$ 24.451,97
			VALOR TOTAL	R\$24.451,97

1.2.1. Havendo mais de item ou lote faculta-se ao prestador a participação em quantos

forem de seu interesse. Entretanto, optando-se por participar de um lote, deve o fornecedor enviar proposta para todos os itens que o compõem.

- 1.3. O critério de julgamento adotado será o *menor preço global*, observadas as exigências contidas neste Aviso de Contratação Direta e seus Anexos quanto às especificações do objeto.

PARTICIPAÇÃO NA DISPENSA ELETRÔNICA.

- 1.4. A participação na presente dispensa eletrônica se dará mediante Sistema de Dispensa Eletrônica integrante do Sistema de Compras do Governo Federal – Comprasnet 4.0, disponível no endereço eletrônico: <https://www.gov.br/compras/pt-br>

- 1.4.1. Os fornecedores deverão atender aos procedimentos previstos no Manual do Sistema de Dispensa Eletrônica, disponível no Portal de Compras do Governo Federal, para acesso ao sistema e operacionalização.

- 1.4.2. O fornecedor é o responsável por qualquer transação efetuada diretamente ou por seu representante no Sistema de Dispensa Eletrônica, não cabendo ao provedor do Sistema ou ao órgão entidade promotor do procedimento a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros não autorizados.

- 1.5. Não poderão participar desta dispensa os fornecedores:

- 1.5.1. que não atendam às condições deste Aviso de Contratação Direta e seu(s) anexo(s);

- 1.5.2. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

- 1.5.3. que se enquadrem nas seguintes vedações:

- a) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;

- b) empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ela necessários;

- c) pessoa física ou jurídica que se encontre, ao tempo da contratação, impossibilitada de contratar em decorrência de sanção que lhe foi imposta;

- d) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

- e) empresas controladoras, controladas ou coligadas, nos termos da [Lei nº 6.404, de 15 de dezembro de 1976](#), concorrendo entre si;

- f) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do aviso, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista

- 1.5.3.1. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo

econômico;

1.5.3.2. aplica-se o disposto na alínea “c” também ao fornecedor que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do fornecedor;

1.5.4. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário); e

2. INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL

2.1. O ingresso do fornecedor na disputa da dispensa eletrônica se dará com o cadastramento de sua proposta inicial, na forma deste item.

2.2. O fornecedor interessado, após a divulgação do aviso de contratação direta, encaminhará, exclusivamente por meio do Sistema de Dispensa Eletrônica, a proposta com a descrição do objeto ofertado, a marca do produto, quando for o caso, e o preço, até a data e o horário estabelecidos para abertura do procedimento.

2.2.1. A proposta também deverá conter declaração de que compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

2.3. Todas as especificações do objeto contidas na proposta, em especial o preço, vinculam a Contratada.

2.4. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços;

2.4.1. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do fornecedor, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

2.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

2.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

2.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o *Termo de Referência*, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

2.8. Uma vez enviada a proposta no sistema, os fornecedores **NÃO** poderão retirá-la, substituí-la ou modificá-la;

2.9. No cadastramento da proposta inicial, o fornecedor deverá, também, assinalar “sim” ou “não” em campo próprio do sistema eletrônico, às seguintes declarações:

2.9.1. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

- 2.9.2. que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.
- 2.9.3. que está ciente e concorda com as condições contidas no Aviso de Contratação Direta e seus anexos;
- 2.9.4. que assume a responsabilidade pelas transações que forem efetuadas no sistema, assumindo como firmes e verdadeiras;
- 2.9.5. que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, de que trata o art. 93 da Lei nº 8.213/91.
- 2.9.6. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;

3. FASE DE LANCES

- 3.1. A partir das 8:05h da data estabelecida neste Aviso de Contratação Direta, a sessão pública será automaticamente aberta pelo sistema para o envio de lances públicos e sucessivos, exclusivamente por meio do sistema eletrônico, sendo encerrado no horário de finalização de lances também já previsto neste aviso.
- 3.2. Iniciada a etapa competitiva, os fornecedores deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.
 - 3.2.1. *O lance deverá ser ofertado pelo valor unitário do item.*
- 3.3. O fornecedor somente poderá oferecer valor inferior ou maior percentual de desconto em relação ao último lance por ele ofertado e registrado pelo sistema.
 - 3.3.1. O fornecedor poderá oferecer lances sucessivos iguais ou superiores ao lance que esteja vencendo o certame, desde que inferiores ao menor por ele ofertado e registrado pelo sistema, sendo tais lances definidos como “lances intermediários” para os fins deste Aviso de Contratação Direta.
 - 3.3.2. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir a melhor oferta é de R\$ 100,00(*cem reais*)
- 3.4. Havendo lances iguais ao menor já ofertado, prevalecerá aquele que for recebido e registrado primeiro no sistema.
- 3.5. Caso o fornecedor não apresente lances, concorrerá com o valor de sua proposta.
- 3.6. Durante o procedimento, os fornecedores serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do fornecedor.
- 3.7. Imediatamente após o término do prazo estabelecido para a fase de lances, haverá o seu encerramento, com o ordenamento e divulgação dos lances, pelo sistema, em ordem crescente de classificação.
 - 3.7.1. O encerramento da fase de lances ocorrerá de forma automática pontualmente no horário indicado, sem qualquer possibilidade de prorrogação e não havendo tempo aleatório ou mecanismo similar.

4. JULGAMENTO DAS PROPOSTAS DE PREÇO

- 4.1. Encerrada a fase de lances, será verificada a conformidade da proposta classificada em primeiro lugar quanto à adequação do objeto e à compatibilidade do preço em relação ao

estipulado para a contratação.

- 4.2. No caso de o preço da proposta vencedora estar acima do estimado pela Administração, poderá haver a negociação de condições mais vantajosas.
 - 4.2.1. Neste caso, será encaminhada contraproposta ao fornecedor que tenha apresentado o melhor preço, para que seja obtida melhor proposta com preço compatível ao estimado pela Administração.
 - 4.2.2. A negociação poderá ser feita com os demais fornecedores classificados, respeitada a ordem de classificação, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido para a contratação.
 - 4.2.3. Em qualquer caso, concluída a negociação, o resultado será registrado na ata do procedimento da dispensa eletrônica.
- 4.3. Estando o preço compatível, será solicitado o envio da proposta e, se necessário, de documentos complementares, adequada ao último lance.
- 4.4. O prazo de validade da proposta não será inferior a 90 (noventa dias) dias, a contar da data de sua apresentação.
- 4.5. Será desclassificada a proposta vencedora que:
 - 4.5.1. contiver vícios insanáveis;
 - 4.5.2. não obedecer às especificações técnicas pormenorizadas neste aviso ou em seus anexos;
 - 4.5.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;
 - 4.5.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;
 - 4.5.5. apresentar desconformidade com quaisquer outras exigências deste aviso ou seus anexos, desde que insanável.
- 4.6. Quando o fornecedor não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:
 - 4.6.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da dispensa não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio fornecedor, para os quais ele renuncie a parcela ou à totalidade da remuneração.
 - 4.6.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.
- 4.7. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.
- 4.8. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.
 - 4.8.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;
 - 4.8.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de

recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

- 4.9. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.
- 4.10. Se a proposta ou lance vencedor for desclassificado, será examinada a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.
- 4.11. Havendo necessidade, a sessão será suspensa, informando-se no “chat” a nova data e horário para a sua continuidade.
- 4.12. Encerrada a análise quanto à aceitação da proposta, se iniciará a fase de habilitação, observado o disposto neste Aviso de Contratação Direta.

5. HABILITAÇÃO

- 5.1. Os documentos a serem exigidos para fins de habilitação constam do **ANEXO I – DOCUMENTAÇÃO EXIGIDA PARA HABILITAÇÃO** deste aviso e serão solicitados do fornecedor mais bem classificado da fase de lances.
- 5.2. Como condição prévia ao exame da documentação de habilitação do fornecedor detentor da proposta classificada em primeiro lugar, será verificado o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:
 - a) SICAF;
 - 5.2.1. Consulta Consolidada de Pessoa Jurídica do TCU (<https://certidoesapf.apps.tcu.gov.br/>)
 - 5.2.2. A consulta aos cadastros será realizada em nome da empresa fornecedora e também de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.
 - 5.2.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.
 - 5.2.2.1.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.
 - 5.2.2.1.2. O fornecedor será convocado para manifestação previamente à sua desclassificação
 - 5.2.3. Constatada a existência de sanção, o fornecedor será reputado inabilitado, por falta de condição de participação.
- 5.3. Caso atendidas as condições de participação, a habilitação dos fornecedores será verificada por meio do SICAF, nos documentos por ele abrangidos.
 - 5.3.1. É dever do fornecedor atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, quando solicitado, a respectiva documentação atualizada.
 - 5.3.2. O descumprimento do subitem acima implicará a inabilitação do fornecedor, exceto

se a consulta aos sítios eletrônicos oficiais emissores de certidões lograr êxito em encontrar a(s) certidão(ões) válida(s).

- 5.4. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Aviso de Contratação Direta e já apresentados, o fornecedor será convocado a encaminhá-los, em formato digital, após solicitação da Administração, sob pena de inabilitação.
- 5.5. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.
- 5.6. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.
- 5.7. Havendo necessidade de analisar minuciosamente os documentos exigidos, a sessão será suspensa, sendo informada a nova data e horário para a sua continuidade.
- 5.8. Será inabilitado o fornecedor que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Aviso de Contratação Direta.
 - 5.8.1. Na hipótese de o fornecedor não atender às exigências para a habilitação, o órgão ou entidade examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações do objeto e as condições de habilitação
- 5.9. Constatado o atendimento às exigências de habilitação, o fornecedor será habilitado

6. CONTRATAÇÃO

- 6.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.
- 6.2. O adjudicatário terá o prazo de 5(cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Aviso de Contratação Direta.
- 6.3. O Termo de Contrato será assinado pela plataforma sei, ao qual será providenciado o cadastramento de usuário externo, para a(s) empresa(s) vencedoras, para seus respectivos representantes.
 - 6.3.1. O prazo previsto para assinatura do contrato ou aceitação da nota de empenho ou instrumento equivalente poderá ser prorrogado 1 (uma) vez, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.
- 6.4. O prazo de vigência da contratação é de 12 meses, não prorrogável conforme previsão nos anexos a este Aviso de Contratação Direta.
- 6.5. Na assinatura do contrato ou do instrumento equivalente será exigida a comprovação das condições de habilitação e contratação consignadas neste aviso, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

7. SANÇÕES

7.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

7.1.1. dar causa à inexecução parcial do contrato;

7.1.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

7.1.3. dar causa à inexecução total do contrato;

7.1.4. deixar de entregar a documentação exigida para o certame;

7.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

7.1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

7.1.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

7.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

7.1.9. fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

7.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

7.1.10.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

7.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste certame.

7.1.12. praticar ato lesivo previsto no [art. 5º da Lei nº 12.846, de 1º de agosto de 2013.](#)

7.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 8.1.1 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

b) Multa de 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor, por qualquer das infrações dos subitens 8.1.1 a 8.1.12;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 8.1.2 a 8.1.7 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.1.8 a 8.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

7.3. Na aplicação das sanções serão considerados:

7.3.1. a natureza e a gravidade da infração cometida;

7.3.2. as peculiaridades do caso concreto;

7.3.3. as circunstâncias agravantes ou atenuantes;

7.3.4. os danos que dela provierem para a Administração Pública;

7.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e

orientações dos órgãos de controle.

7.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

7.5. A aplicação das sanções previstas neste Aviso de Contratação Direta, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

7.6. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

7.7. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

7.8. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

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

7.10. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133, de 2021, e subsidiariamente na Lei nº 9.784, de 1999.

7.11. As sanções por atos praticados no decorrer da contratação estão previstas nos anexos a este Aviso.

8. DAS DISPOSIÇÕES GERAIS

8.1. O procedimento será divulgado no Comprasnet 4.0 e no Portal Nacional de Contratações Públicas - PNCP, e encaminhado automaticamente aos fornecedores registrados no Sistema de Registro Cadastral Unificado - Sicaf, por mensagem eletrônica, na correspondente linha de fornecimento que pretende atender.

8.2. No caso de todos os fornecedores restarem desclassificados ou inabilitados (procedimento fracassado), a Administração poderá:

8.2.1. republicar o presente aviso com uma nova data;

8.2.2. valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando-se os menores preços, sempre que possível, e desde que atendidas às condições de habilitação exigidas.

8.2.2.1. No caso do subitem anterior, a contratação será operacionalizada fora deste procedimento.

8.2.3. fixar prazo para que possa haver adequação das propostas ou da documentação de habilitação, conforme o caso.

8.3. As providências dos subitens 9.2.1 e 9.2.2 acima poderão ser utilizadas se não houver o comparecimento de quaisquer fornecedores interessados (procedimento deserto)

8.4. Havendo a necessidade de realização de ato de qualquer natureza pelos fornecedores,

cujo prazo não conste deste Aviso de Contratação Direta, deverá ser atendido o prazo indicado pelo agente competente da Administração na respectiva notificação.

8.5. Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pela Administração ou de sua desconexão.

8.6. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário.

8.7. Os horários estabelecidos na divulgação deste procedimento e durante o envio de lances observarão o horário de Brasília-DF, inclusive para contagem de tempo e registro no Sistema e na documentação relativa ao procedimento.

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

8.9. As normas disciplinadoras deste Aviso de Contratação Direta serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

8.10. Os fornecedores assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo de contratação.

8.11. Em caso de divergência entre disposições deste Aviso de Contratação Direta e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Aviso.

8.12. Da sessão pública será divulgada Ata no sistema eletrônico.

8.13. Integram este Aviso de Contratação Direta, para todos os fins e efeitos, os seguintes anexos:

8.13.1. ANEXO I – Documentação exigida para Habilitação

8.13.2. ANEXO II - *Estudo Técnico Preliminar*;

8.13.3. ANEXO II.1 – Termo de Referência;

8.13.4. ANEXO III – *Minuta de Termo de Contrato*;

Goiânia, 15/10/2024

ANEXOS À MINUTA DE EDITAL

ANEXO I – DOCUMENTAÇÃO EXIGIDA PARA HABILITAÇÃO

1 Habilitação jurídica:

1.1 no caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

1.2 Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação

da autenticidade no sítio www.portaldoempreendedor.gov.br;

- 1.3 No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;
- 1.4 inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;
- 1.5 No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;
- 1.6 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

2 Regularidade fiscal, social e trabalhista:

- 2.1 prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
- 2.2 prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
- 2.3 prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 2.4 prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;
- 2.5 prova de inscrição no cadastro de contribuintes *estadual e municipal*, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 2.6 prova de regularidade com a Fazenda *Estadual e Municipal* do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 2.7 caso o fornecedor seja considerado isento dos tributos *estaduais* **ou** *municipais* relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei;

3 Qualificação Econômico-Financeira:

- 3.1 certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

4 Qualificação Técnica

- 4.1 Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta dispensa, ou com o item pertinente, mediante a apresentação de atestado (s) fornecido(s) por pessoas jurídicas de direito público ou privado.

4.1.1.1 Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

4.1.1.2 O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.



Documento assinado eletronicamente por **Admilton Marques da Silva, Assistente**, em 15/10/2024, às 10:10, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0549977** e o código CRC **D14BB614**.