CONTRATO Nº 49/2023

Contrato que entre si celebram a **CÂMARA MUNICIPAL DE GOIÂNIA** e a empresa **JRV SERVIÇOS LTDA-ME (XLOGIC SOLUÇÕES EM TI)**, nas cláusulas e condições que se seguem:

A CÂMARA MUNICIPAL DE GOIÂNIA, com sede em Goiânia, Capital do Estado de Goiás, situada na Avenida Goiás Norte, nº 2001, Centro - CEP nº 74.063-900 inscrita no CNPJ/MF sob o nº 00.001.727/0001-93, doravante designada simplesmente **CONTRATANTE**, neste ato representada pelo Diretor Financeiro, Vitor Pessoa Loureiro de Morais, brasileiro, inscrito no CPF sob o n.º 030.542.931-06, em conformidade com as Portarias nº 219/2017 e 918/2022, e a empresa **JRV SERVIÇOS LTDA-ME (XLOGIC SOLUÇÕES EM TI),** pessoa jurídica de direito privado, sediada na Avenida Tancredo Neves, nº 620, Edifício Mundo Plaza Torre Empresarial, Salas 2105 e 2106, Caminho das Árvores, Salvador/BA , CEP 41.820-020, inscrita no CNPJ/MF, sob o nº 08.208.805/0001-37, neste ato representada, na forma do seu Contrato Social, por seu Sócio, Diretor Comercial, Sr. Antônio Vicente Barbosa do Vale, inscrito no CPF sob o n° 799.492.745-91, RG 6.352.229-22, doravante denominada apenas **CONTRATADA,** têm entre si justo e avençado, e celebram o presente Contrato de fornecimento de Solução de Segurança NGFW, em conformidade com o disposto nas Leis 10.520/02, 8.666/93, Decreto Federal nº 10.024/2019 e demais legislações pertinentes, de acordo com as condições e especificações estabelecidas no Edital do Pregão Eletrônico n° 34/2022, conforme Ofício Homologatório nº 711/2023 – DRFIN/MSDIR/PLENA/CMG e nos termos da documentação contida no Processo Eletrônico n° 00000.03686.2022-12, e mediante as seguintes cláusulas e condições:

1. CLÁUSULA PRIMEIRA – DO OBJETO DO CONTRATO

1.1 - Constitui objeto do presente contrato o fornecimento de Solução de Segurança NGFW com Subscrição e Produto, incluindo instalação, capacitação técnica, garantia e suporte, visando atender as necessidades da Câmara Municipal de Goiânia, conforme condições e especificações estabelecidas neste Contrato, no Edital do Pregão Eletrônico nº 34/2022 e seus Anexos.

1.2 - DA ESPECIFICAÇÃO DOS PRODUTOS:

1.2.1 - Os produtos ora contratados foram objeto de licitação, de acordo com o disposto no art. 1° e parágrafo único da Lei n° 10.520/2002, sob a modalidade de Pregão Eletrônico, conforme especificações constantes na planilha abaixo:

ITEM	DESCRIÇÃO	UND.	QTD.	PREÇO UNITÁRIO	VALOR TOTAL
1	Solução Next Generation Firewall (HARDWARE) Marca: FORTINET; Origem: USA; Modelo: FORTIGATE- FG 200F.	UND	02	R$ 50.700,00	R$ 101.400,00
2	Software e Licenciamento para Firewall / treinamento e migração. Marca: FORTINET; Origem: USA; Part Number FC-10-F200F-950-02-36.	UND	02	R$ 97.500,00	R$ 195.000,00
3	Appliance (Virtual — Software) especializado na coleta e armazenamento de logs. Marca: FORTINET ; Origem:USA FORTIANALYZER AZ-VM-GB25 Part Number FC3-10-LV0VM-248-02-36.	UND	01	R$ 93.600,00	R$ 93.600,00
VALOR TOTAL:				**R$ 390.000,00 (trezentos e noventa mil reais).**	

2. CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATADA:

2.1 - Não transferir a outrem, no todo ou em parte, o presente Contrato;

2.2 - Prestar o serviço contratado, obedecendo às quantidades, especificações, prazos e condições constantes neste Instrumento e seu Anexo Único, no Termo de Referência, no Edital do Pregão Eletrônico n° 034/2022, bem como na proposta ofertada pela CONTRATADA;

2.3 - Fornecer, além dos equipamentos especificados e mão de obra especializada, todas as ferramentas necessárias para a instalação dos produtos, ficando responsável por sua guarda e transporte;

2.4 - Responder pela qualidade dos produtos oferecidos, que deverão ser compatíveis com as finalidades a que se destinam, bem como pelo fornecimento ou eventuais atrasos;

2.5 - Responder por perdas e danos que vier a causar à CONTRATANTE ou a terceiros, em razão de ação ou omissão, dolosa ou culposa, sua ou de seus prepostos, independentemente de outras cominações contratuais ou legais, a que estiver sujeita, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento realizado pela CONTRATANTE;

2.6 - Ressarcir os eventuais prejuízos causados à CONTRATANTE e/ou a terceiros, provocados por ineficiência ou irregularidades cometidas no fornecimento do objeto contratado;

2.7 - Corrigir e/ou refazer os serviços e substituir os produtos não aprovados pela Fiscalização ou que apresente defeito, caso os mesmos não atendam às especificações constantes do Termo de Referência ou às normas pertinentes, ficando a Câmara isenta de despesas;

2.8 - Responsabilizar-se por todas as despesas diretas ou indiretas, tais como: mão de obra, material, tributos, serviços de terceiros, salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras que forem devidas aos seus empregados no desempenho do fornecimento objeto do contrato, ficando a CONTRATANTE isenta de qualquer vínculo;

2.9- Prestar esclarecimentos que lhe forem solicitados, atendendo prontamente às eventuais reclamações relacionadas com o produto fornecido;

2.10 - Manter, durante a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, em consonância com o disposto no artigo 55, inciso XIII da Lei n° 8.666/93;

2.11 - Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

2.12 - Propiciar todos os meios e facilidades necessários à fiscalização da Solução de Tecnologia da Informação pela CONTRATANTE, cujo representante terá poderes para sustar

o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

2.13 - Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação;

2.14 - Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato;

2.15 - Fornecer, sempre que solicitado, amostra para realização de Prova de Conceito para fins de comprovação de atendimento das especificações técnicas;

2.16 - Ceder, quando for o caso, os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, à Administração.

3. CLÁUSULA TERCEIRA – A CONTRATANTE FICA COMPROMETIDA A:

3.1 - Verificar e fiscalizar as condições técnicas da CONTRATADA, visando estabelecer controle de qualidade dos produtos a serem fornecidos e da garantia a ser prestada;

3.2 - Fiscalizar, gerenciar e monitorar todas as atividades decorrentes do fornecimento e garantia, por meio do servidor ocupante do cargo de Diretor de Tecnologia da Informação.

3.3 - Efetuar o pagamento à CONTRATADA no valor e época estabelecidos na Cláusula Quinta;

4. CLÁUSULA QUARTA – DO PRAZO DE VIGÊNCIA E DA ASSINATURA DO CONTRATO

4.1 - O contrato a ser celebrado terá vigência de **12 (doze) meses,** contados da data da assinatura;

4.2 - O período de 36 (trinta e seis) meses de garantia se refere à vigência das licenças de software e da garantia, incluindo suporte no formato 8x5 (oito horas, cinco dias por semana em horário comercial) com troca de equipamentos e peças que demonstrem mal

funcionamento em até 24 horas úteis. A referida garantia e suporte não implicam em custo futuro à contratante;

4.3 - Considera-se válida a assinatura digital utilizando sistema eletrônico com senha pessoal e intransferível, capaz de comprovar a autoria e integridade do documento;

4.4 - No caso de assinatura digital, o prazo de vigência contratual iniciará a partir da data do último registro eletrônico, que coincidirá com a data da celebração do presente instrumento.

5. CLÁUSULA QUINTA – DO PREÇO E DA FORMA DE PAGAMENTO

5.1 - DO PREÇO: A CONTRATANTE pagará a CONTRATADA o valor referente ao fornecimento do objeto, no valor total de **R$ 390.000,00 (trezentos e noventa mil reais).**

5.1.1 - Nos preços estipulados estão incluídos todos os custos decorrentes do fornecimento do objeto tais como: mão de obra, salário, encargos sociais, fiscais, previdenciários, de segurança do trabalho e trabalhistas, fretes, seguros, impostos e taxas, contribuições e alvarás, ou quaisquer outros custos incidentes diretos ou indiretos, mesmo não especificados e que sejam necessários à consecução deste, inclusive benefícios, taxa de administração e lucro.

5.2 - DA FORMA DE PAGAMENTO: O pagamento será efetuado, até o 10° (décimo) dia do mês subsequente ao do fornecimento/execução, por meio de ordem de Pagamento, mediante apresentação da respectiva fatura discriminativa, após devida atestação, via Ordem de Pagamento no Banco do Brasil Agência 3025-2 C/C: 16968-4.

5.2.1 - Nenhum pagamento será efetuado à CONTRATADA, enquanto perdurarem eventuais multas que tenham sido impostas à CONTRATADA em virtude de penalidades ou inadimplência.

5.3 - ATRASO DE PAGAMENTO: Sobre os valores das faturas não quitadas na data de seus respectivos vencimentos, incidirá juros de 0,5% (meio por cento) a.m., *pro rata die*, desde que solicitado pela CONTRATADA.

6. CLÁUSULA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta das seguintes dotações orçamentárias:

a) nº **2023.0101.01.031.0001.1458.44905235.100.501.1500.0,** conforme Nota de Empenho nº **0013 00**, no valor de **R$ 101.400,00 (cento e um mil e quatrocentos reais)**, datada em **17/10/2023,** referente à aquisição de 02 (dois) equipamentos de *hardware*;
b) nº **2023.0101.01.031.0001.2001.33904003.100.501.1500.0,** conforme Nota de Empenho nº **0026 00**, no valor de **R$ 288.600,00 (duzentos e oitenta e oito mil e seiscentos reais)**, datada em **17/10/2023,** referente à aquisição de *software* e licenciamento para *firewall*, treinamento e migração, bem como de *software appliance.*

7. CLÁUSULA SÉTIMA – DAS PENALIDADES E MULTA

7.1 - Pela inexecução total ou parcial do objeto do Pregão Eletrônico nº 34/2022, a CONTRATANTE poderá garantida a prévia defesa, aplicar à CONTRATADA as seguintes sanções:

7.1.1 Advertência, que será aplicada através de notificação por meio de ofício, mediante contra-recibo do representante legal da contratada estabelecendo o prazo de 05 (cinco) dias úteis para que a CONTRATADA apresente justificativas para o atraso, que só serão aceitas mediante crivo da CÂMARA MUNICIPAL DE GOIÂNIA;

7.1.2 - Multa de 0,5% (meio por cento) por dia de atraso no fornecimento dos produtos, calculada sobre o valor do produto não entregue, até o máximo de 10 (dez) dias, quando então incidirá em outras cominações legais;

7.1.3- Multa de 2% sobre o valor do contrato, no caso de inexecução total ou parcial do objeto contratado, recolhida no prazo de 15 (quinze) dias corridos, contado da comunicação oficial, sem embargo de indenização dos prejuízos porventura causados a contratante, com o não fornecimento parcial ou total do contrato;

7.1.4 - A multa, aplicada após regular processo administrativo, será descontada da garantia do respectivo contrato;

7.1.5 - Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente;

7.2 - Ficará impedida de licitar e de contratar com a Administração Pública:

7.2.1 - Por 06 (seis) meses – quando incidir em atraso no fornecimento dos produtos;

7.2.2 - Por 01 (um) ano – no fornecimento dos produtos em desacordo com o exigido em contrato;

7.2.3 - Pelo prazo de até 05 (cinco) anos, garantido o direito prévio da citação e de ampla defesa, a licitante que convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida para o certame ou

apresentar documentação falsa, ensejar o retardamento do fornecimento dos produtos, não mantiver a proposta, falhar ou fraudar no fornecimento do objeto pactuado, comportar-se de modo inidôneo ou cometer fraude fiscal.

7.3 - As sanções previstas no subitem 7.1 poderão ser aplicadas juntamente com as do subitem 7.2 facultados a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis.

7.4 - Em conformidade com o artigo 7° da Lei n° 10.520/2002 - Ficará impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e será descredenciado no cadastro de fornecedores deste Município pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas no Edital e neste Contrato e das demais cominações legais o licitante que:

7.4.1 - Convocado dentro do prazo de validade da Proposta de Preços e não celebrar o contrato;

7.4.2 - Deixar de entregar documentação exigida para o certame dentro do prazo estabelecido no Edital, considerando, também, como documentação a proposta ajustada;

7.4.3 - Apresentar documentação falsa exigida para o certame;

7.4.4 - Comportar-se de modo inidôneo ou cometer fraude fiscal;

7.4.5 - Ensejar retardamento da execução de seu objeto;

7.4.6 - Não mantiver a proposta;

7.4.7 - Falhar ou fraudar na execução do contrato.

7.5 - Pelo descumprimento das demais obrigações assumidas, a licitante estará sujeita às penalidades previstas na Lei n.º 8.666/1993 e demais legislações aplicáveis à espécie;

7.6 - Por infração a quaisquer outras cláusulas contratuais, será aplicada multa de até 2% (dois por cento) sobre o valor total do Contrato atualizado, cumuláveis com as demais sanções, inclusive rescisão contratual, se for o caso;

7.7 - Se o valor da multa não for pago, ou depositado, será automaticamente descontado da primeira parcela do preço a que fizer *jus*. Em caso de inexistência ou insuficiência de crédito da Contratada, o valor devido será cobrado administrativamente e/ou inscrito como Dívida Ativa do Município de Goiânia e cobrado judicialmente;

7.8 - Para garantir o fiel pagamento da multa, reserva-se o direito de reter o valor contra qualquer crédito gerado pela CONTRATADA, independentemente de notificação judicial ou extrajudicial.

8. CLÁUSULA OITAVA – DO FORNECIMENTO/PRESTAÇÃO DOS SERVIÇOS

8.1- A CONTRATADA deverá fornecer/prestar os serviços contratados nos quantitativos solicitados pela CONTRATANTE, conforme prescrito no Termo de Referência do Pregão Eletrônico nº 34/2022 e Anexo I do Edital;

8.1.1 - O responsável pelo recebimento do objeto/serviço deverá atestar a qualidade e quantidade dos serviços, mediante recibo (§1º do art. 73), devendo rejeitar qualquer serviço que esteja em desacordo com o especificado no Edital;

8.2 - A CONTRATADA deverá efetuar o fornecimento/prestação dos serviços em perfeitas condições conforme a proposta apresentada, dentro do horário e local estabelecido pela CONTRATANTE;

8.3 - Quando a licitante vencedora não apresentar situação regular no ato da assinatura do contrato ou recusar-se a assiná-lo, será convocado outro licitante, observadas a ordem de classificação e as exigências habilitatórias constantes do edital, para celebrar o contrato, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis;

8.4 - Em conformidade com os artigos 73 e 76 da Lei n.º 8.666/93, mediante recibo, o objeto deste Contrato será recebido:

I - Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita do contratado;

II - Definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de 05 (cinco) dias úteis a contar da solicitação do CONTRATANTE, depois de passado a observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no art. 69 da Lei nº 8.666/93.

8.4.1 - Se, após o recebimento provisório, constatar-se que os materiais/serviços foram prestados em desacordo com a proposta, com defeito, fora da especificação ou incompletos, após a notificação por escrito à adjudicatária serão interrompidos os prazos de recebimento e suspenso o pagamento, até que sanada a situação.

8.4.2 - O recebimento provisório ou definitivo não exime a responsabilidade da adjudicatária *a posteriori*. Deverão ser substituídos os materiais/serviços que, eventualmente, não atenderem as especificações do Edital.

9. CLÁUSULA NONA – DA RESCISÃO

9.1 - A inexecução total ou parcial deste Contrato enseja sua rescisão, com as consequências contratuais, inclusive o reconhecimento dos direitos da Câmara Municipal de Goiânia, conforme disposto nos artigos 77 e 80 da Lei 8.666/93 e posteriores alterações;

9.2 - A rescisão poderá ser:

9.2.1 – Determinada, por ato unilateral e escrito da Câmara Municipal de Goiânia, nos casos enumerados nos incisos I a XII e XVII e XVIII do artigo 78 da sobredita Lei;

9.2.2 - Amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para a Câmara Municipal de Goiânia;

9.2.3 - Judicial, nos termos da legislação;

9.3 - Os casos de rescisão serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa;

9.4 - A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

10. CLÁUSULA DÉCIMA – DA GARANTIA

10.1 - A CONTRATANTE exigirá da CONTRATADA em até 60 dias da data da assinatura do Contrato, prestação de garantia, correspondente a 3% (três por cento) do valor do contrato, ficando facultado ao contratado optar por uma das seguintes modalidades:

10.1.1 - Caução em dinheiro, ou em títulos da dívida pública;

10.1.1.1 - Caução em dinheiro ou em títulos da dívida pública deverá ser depositado em uma conta da Caixa Econômica Federal, vinculada à Câmara Municipal de Goiânia. O licitante vencedor deverá se dirigir à Diretoria Financeira da Câmara Municipal de Goiânia, Av. Goiás, nº 2001, Centro – Goiânia – Goiás, fones: (62) 3524-4226/4227, para obterem esclarecimentos sobre o referido recolhimento;

10.1.1.2 - Os Títulos da Dívida Pública deverão ser emitidos sob forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos valores econômicos, conforme definido pelo Ministério da Fazenda.

10.1.2- Seguro-garantia;

10.1.2.1 - Caso o licitante vencedor preste garantia por meio de Seguro-garantia, deverá juntar o comprovante de pagamento do prêmio;

10.1.3 - Fiança Bancária.

10.1.3.1 - A fiança bancária formalizar-se-á através de carta de fiança fornecida por instituição financeira que, por si ou pelos acionistas detentores de seu controle,não participem do capital ou da direção da CONTRATADA;

10.1.3.2- Em se tratando de fiança bancária, deverá constar do Instrumento a expressa renúncia pelo fiador dos benefícios previstos nos arts. 827 e 835 do Código Civil. A contratada que optar por recolhimento em Seguro-Garantia e Fiança Bancária, deverá apresentá-la à Diretoria Financeira da Câmara Municipal de Goiânia, Av. Goiás, nº 2001, Centro – Goiânia – Goiás, fones: (62) 3524-4226/4227, para obterem esclarecimentos sobre o referido recolhimento;

10.2 - A garantia prestada pelo contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente;

10.3 - A garantia poderá, a critério da Administração, ser utilizada para cobrir eventuais multas e/ou para cobrir o inadimplemento de obrigações contratuais, sem prejuízo da indenização eventualmente cabível. Nesta hipótese, no prazo máximo de 15 (quinze) dias corridos após o recebimento da notificação regularmente expedida, a garantia deverá ser reconstituída;

10.4 - A garantia ficará retida no caso de rescisão contratual, até definitiva solução das pendências administrativas ou judiciais;

10.5 - Sem prejuízo das sanções previstas na lei e no Edital, a não prestação da garantia exigida será considerada recusa injustificada em assinar o Contrato, implicando na imediata anulação da Nota de Empenho emitida ou documento equivalente;

10.6 - A garantia será restituída, somente, após o integral cumprimento de todas as obrigações contratuais, inclusive recolhimento de multas e satisfação de prejuízos causados à CONTRATANTE;

10.7 - Quando a rescisão ocorrer com base nos incisos XII a XVII do artigo 78, da Lei 8.666/93, sem que haja culpa da contratada, será devolvida a caução.

11. CLÁUSULA DÉCIMA PRIMEIRA – DA PUBLICAÇÃO

Caberá a CONTRATANTE providenciar, por sua conta, a publicação resumida do Instrumento de Contrato e de seus aditamentos, na imprensa oficial e no prazo legal, conforme o art. 61, parágrafo único, da Lei 8.666/93.

12. CLÁUSULA DÉCIMA SEGUNDA – DA APRECIAÇÃO DA CONTROLADORIA GERAL DA CÂMARA MUNICIPAL DE GOIÂNIA E DO ENVIO AO TRIBUNAL DE CONTAS DOS MUNICÍPIOS DO ESTADO DE GOIÁS.

O presente Instrumento será objeto de apreciação pela Controladoria Geral da Câmara Municipal de Goiânia e enviado no site do Tribunal de Contas dos Municípios do Estado de Goiás – TCM/GO, via plataforma COLARE, em até 03 (três) dias úteis a contar da publicação oficial, com respectivo *upload* do arquivo correspondente, de acordo com a IN nº 12/18 do TCM/GO, não se responsabilizando o CONTRATANTE, se aquela Corte de Contas, por qualquer motivo, denegar-lhe aprovação.

13. CLÁUSULA DÉCIMA TERCEIRA – DOS TRIBUTOS

A CONTRATADA será responsável exclusiva por todos e quaisquer tributos e encargos trabalhistas, sociais e previdenciários, decorrentes do fornecimento dos produtos, objeto da licitação, e qualquer outro necessário à adequada execução do objeto da licitação.

14. CLÁUSULA DÉCIMA QUARTA – DA VINCULAÇÃO

Consideram-se integrantes do presente instrumento contratual, os termos do Edital do Pregão Eletrônico n° 034/2022 e seus Anexos, a Proposta da CONTRATADA datada de **14/09/2023**, e demais documentos pertinentes, independentemente de transcrição.

15. CLÁUSULA DÉCIMA QUINTA – DA GESTÃO e DA FISCALIZAÇÃO CONTRATUAL

15.1 - Em atendimento aos arts. 58, III, e 67, § 1°, da Lei Federal nº 8.666/93, juntamente com o art. 16, XX, da Instrução Normativa n° 015/2012, e com o art. 3°, XXI, da Instrução Normativa n° 010/2015, ambas do Tribunal de Contas dos Municípios do Estado de Goiás e, de acordo com o art. 15, I a XI e art. 17, I a XXII e parágrafos, da Portaria nº 283, de 27/02/2023, a execução do Contrato será acompanhada e fiscalizada por representantes da CÂMARA MUNICIPAL DE GOIÂNIA, especialmente designados para a gestão e fiscalização contratual;

15.2 - A gestão do presente Instrumento Contratual caberá a Comissão Gestora de Contratos, nomeada pela Portaria nº 847, de 29/06/2023, tendo a Diretoria Geral como suporte técnico e operacional;

15.3 - A função de fiscal do Contrato caberá ao servidor ocupante do cargo de Diretor de Tecnologia da Informação.

16. CLÁUSULA DÉCIMA SEXTA – DAS DISPOSIÇÕES GERAIS

Aos casos omissos, aplicar-se-á as demais disposições da Lei n° 10.520/02 e Lei federal n° 8.666/93 e alterações posteriores.

17. CLÁUSULA DÉCIMA SÉTIMA – DO FORO

Para as questões resultantes do instrumento, fica eleito o Foro da Comarca de Goiânia, Município de Goiânia, com renúncia expressa a qualquer outro, por mais privilegiado que seja ou venha a se tornar.

E por estarem assim justas e acordadas, as partes assinam o presente instrumento, em 02 (duas) vias de igual teor e forma para um só efeito legal, na presença das testemunhas abaixo nominadas.

Goiânia-GO, data da última assinatura eletrônica.

Pela CONTRATANTE:

ASSINADO DIGITALMENTE
VITOR PESSOA LOUREIRO DE MORAIS
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

Vitor Pessoa Loureiro de Morais
CÂMARA MUNICIPAL DE GOIÂNIA

Pela CONTRATADA

gov.br
Documento assinado digitalmente
ANTONIO VICENTE BARBOSA DO VALE
Data: 01/11/2023 10:49:45-0300
Verifique em https://validar.iti.gov.br

Antônio Vicente Barbosa do Vale
JRV SERVIÇOS LTDA-ME (XLOGIC SOLUÇÕES EM TI)

Testemunhas:

1) _____
Nome:
RG:
CPF:

2) _____
Nome:
RG:
CPF:

gov.br
Documento assinado digitalmente
RICARDO CARVALHO RIOS
Data: 01/11/2023 10:57:47-0300
Verifique em https://validar.iti.gov.br

ANEXO ÚNICO – DAS ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS

Neste anexo estão especificados os requisitos mínimos e obrigatórios para todos os itens do escopo de fornecimento, onde a licitante deverá apresentar documentação comprobatória do atendimento de todos os requisitos, bem como deve ainda:

- Apresentar garantias de que os produtos ofertados são de origem comprovada e que possuem garantia do fabricante no território nacional;

- Apresentar documentação técnica (manuais, catálogos oficiais do fabricante) comprovando o pleno atendimento a todos os requisitos técnicos, por meio de apresentação de uma planilha ponto a ponto, com indicação de nome do documento e página que comprova o atendimento. Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante;

- A CONTRATANTE poderá a qualquer momento realizar diligência para comprovação da veracidade de qualquer documento apresentado.

LOTE 01

ITEM 1 - SOLUÇÃO Next Generation Firewall (HARDWARE) (Quantidade: 2) :

1. Throughput de, no mínimo, 25 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 somente (pacote de 1518 byte, UDP);
2. Suporte a, no mínimo, 2,9 milhões conexões simultâneas;
3. Suporte a, no mínimo, 260 mil novas conexões por segundo;
4. Throughput de, no mínimo, 12 Gbps de VPN IP-Sec;
5. Estar licenciado para, ou suportar sem o uso de licença, 15 mil túneis de clientes VPN IPSEC simultâneos;
6. Throughput de, no mínimo, 1,8 Gbps de VPN SSL;
7. Suporte a, no mínimo, 450 clientes de VPN SSL simultâneos;
8. Suportar no mínimo 3,6 Gbps de throughput de IPS;
9. Suporte a, no mínimo, 10 Gbps de throughput de Application Control (Controle de Aplicação);
10. Throughput de, no mínimo, 2,9 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware, filtragem de URL;

11. Throughput de no mínimo 3,9 Gbps para a inspeção de tráfego criptografado (SSL Inspection);
12. Suportar no mínimo 290.000 conexões simultâneas de inspeção de tráfego criptografado (SSL Inspection);
13. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
14. Possuir ao menos 14 interfaces RJ45 1Gbps;
15. Possuir ao menos 6 interfaces 1 GE SFP;

ITEM 2 - SOFTWARE E LICENCIAMENTO PARA FIREWALL (Quan1dade: até 02 dependendo do tipo de licenciamento) :

1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de NextGenera2on Firewall (NGFW) e SDWAN, não sendo permitido appliances virtuais ou solução open source (produto montado/integrado fora de fábrica);
2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;
4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
5. Deve suportar o uso de tabelas de roteamento virtuais (VRF);
6. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada;
7. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
8. Deve possuir suporte a Vlans;
9. Deve suportar BGP, OSPF, RIP e roteamento estático;
10. Deve possuir suporte a DHCP Relay;
11. Deve possuir suporte a DHCP Server;
12. Deve suportar sub-interfaces ethernet logicas;
13. Deve suportar NAT dinâmico (Many-to-Many);
14. Deve suportar NAT estático (1-to-1);
15. Deve suportar NAT estático bidirecional 1-to-1;
16. Deve suportar Tradução de porta (PAT);
17. Deve suportar NAT de Origem;
18. Deve suportar NAT de Destino;
19. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

20. Deve implementar Network Prefix Transla2on (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
21. Deve suportar NAT64;
22. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
23. Enviar log para sistemas de monitoração externos (syslog);
24. Proteção anti-spoofing;
25. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
26. Deve suportar Modo Camada - 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
27. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
28. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo layer 3;
29. A configuração em alta disponibilidade deve sincronizar: sessões, configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede e associações de Segurança das VPNs;
30. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
31. Não serão aceitas soluções baseadas em PCs ("Personal Computer" ou Computador Pessoal) de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
32. Deverá suportar políticas de controles por zonas de segurança;
33. Deverá suportar políticas por porta e protocolo;
34. Deverá suportar políticas de controles por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
35. Controle de políticas por usuários, grupos de usuários, Ips, redes e zonas de segurança;
36. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU) /Geolocalização;
37. Controle, inspeção e descriptografia de SSL por política para tráfego;
38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
39. Suporte a objetos e regras IPV6;
40. Suporte a objetos e regras multicast;
41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré definidos automaticamente;
42. Deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

43. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

44. Reconhecer aplicações por categoria, no mínimo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

45. Reconhecer pelo menos as seguintes aplicações: bijorrent, gnutella, skype, facebook, linked-in, twijer, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, hjp-proxy, hjp-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, Idap, radius, itunes, dhcp, Qp, dns, wins, msrpc, ntp, snmp, rpc over hjp, gotomeeting, webex, evernote, google-docs;

46. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais corno utilização da rede Tor;

47. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

48. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

49. Identificar o uso de táticas evasivas via comunicações criptografadas;

50. Atualizar a base de assinaturas de aplicações automaticamente;

51. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente nas estações dos usuários;

52. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

53. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

54. Deve possuir a capacidade de alertar o usuário quando uma aplicação for bloqueada.

55. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bijorrent, emule etc.) possuindo granularidade de controle/políticas para os mesmos;

56. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat etc.) possuindo granularidade de controle/ políticas para os mesmos;

57. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts (bate papo) e bloquear a chamada de vídeo;

58. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

59. Para proteção do ambiente contra ataques, os disposi2vos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

60. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

61. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

62. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e notificar (log), bloquear o IP do atacante por um intervalo de tempo e/ou definitivamente;

63. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

64. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

65. Deve permitir o bloqueio de exploits conhecidos;

66. Deve incluir proteção contra-ataques de negação de serviços (DoS);

67. Deve ser capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

68. Detectar e bloquear a origem de portscans (varreduras de portas);

69. Possuir assinaturas para bloqueio de ataques do tipo buffer overflow;

70. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

71. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

72. Identificar e bloquear comunicação com botnets;

73. Registrar na console de monitoração as seguintes informações sobre ameaças iden2ficadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

74. Os eventos devem identificar o país de onde partiu a ameaça (Geolocalização/GeolP);

75. Possuir proteção contra downloads usando HTTP de arquivos executáveis e maliciosos;

76. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseados em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

77. Permitir especificar políticas por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

78. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

79. Deve possuir a função de exclusão de URLs do bloqueio (exceções);

80. Permitir a customização de página de bloqueio;

81. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local;

82. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/polí2cas baseadas em usuários e grupos de usuários;

83. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2016 R2 e versões posteriores;

84. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

85. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em usuários e grupos de usuários;

86. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em Usuários e Grupos de usuários;

87. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Cap2ve Portal/Web login) respeitando os quantitativos mínimos de usuários especificados individualmente nos itens;

88. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e MicrosoQ Terminal Server (RDS), permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

89. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados sobre protocolos (HTTP, FTP, SMTP etc.);

90. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

91. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

92. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

93. Suportar VPN Site-to-Site e Cliente-To-Site;

94. Suportar IPSec VPN;

95. Suportar SSL VPN;
96. A VPN IPSEC deve suportar 3DES;
97. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
98. A VPN IPSEc deve suportar Diffie-Hellman Group1, Group 2, Group 5 e Group 14;
99. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
100. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
101. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;
102. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
103. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
104. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
105. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN;
106. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
107. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8/8.1 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.14 ou superior).

ITEM 3 - Appliance (Virtual — Software) especializado na coleta e armazenamento de logs (Quantidade: 1):

1. Capacidade para retenção dos dados pelo período mínimo de 180 dias, além de licenciamento para suportar volume diário ilimitado de coleta e armazenamento de logs;
2. A solução deverá permitir a completa integração com a solução Firewall (ÍTENS 01 e 02). Tal integração deverá ser NATIVA E SEM ADAPTAÇÕES. Esta integração deverá permitir a coleta e o armazenamento de todos os eventos de segurança gerados pela solução de Firewall;
3. Deverá ser baseada em Appliance Virtual (SoQware), suportando a instalação no mínimo em Hypervisores VMware e Hyper- V. Deverá suportar o uso em plataformas nuvem (no mínimo: Azure, AWS, Google). A escolha de Appliance Virtual se deve ao fato de permitir o incremento da volumetria de armazenamento sem custos adicionais;
4. Deverá possuir mecanismos de acesso e gerenciamento através de interfaces do usuário (GUI) de forma gráfica baseada em padrão "WEB" (HTTPS), sendo que para o acesso deverá ser exigido a autenticação via usuário e senha, esta interface deverá ser preferencialmente em língua portuguesa e em casos excepcionais será aceita em língua inglesa;
5. Deverá possuir "Dashboard" gráfico com no mínimo as seguintes informações: informações do sistema, status, alertas e informações de licenciamento;

6. Deverá possuir suporte a SNMP (v2 e v3);

7. Deverá permitir acesso via SSH solicitando usuário e senha;

8. Deverá permitir a exportação dos logs para uso em outras plataformas (suporte a Syslog, exportação CSV e CEF -Common Event Format);

9. Deverá oferecer suporte na modalidade 24 x 7 x 365.

Goiânia-GO, data da última assinatura eletrônica.

Pela CONTRATANTE:

ASSINADO DIGITALMENTE
VITOR PESSOA LOUREIRO DE MORAIS
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

Vitor Pessoa Loureiro de Morais
CÂMARA MUNICIPAL DE GOIÂNIA

Pela CONTRATADA

gov.br
Documento assinado digitalmente
ANTONIO VICENTE BARBOSA DO VALE
Data: 01/11/2023 10:48:11-0300
Verifique em https://validar.iti.gov.br

Antônio Vicente Barbosa do Vale
JRV SERVIÇOS LTDA-ME (XLOGIC SOLUÇÕES EM TI)

CÂMARA MUNICIPAL DE GOIÂNIA | ESTADO DE GOIÁS PODER LEGISLATIVO

Diretoria Geral

CERTIFICAÇÃO 120/2023 - DRGER/MSDIR/PLENA/CMG

Goiânia, 9 de novembro de 2023.

Na condição de testemunhas, conforme autorização prevista no parágrafo único, do art. 30, da Portaria nº 1.206, de 04/10/2022, certificamos para os devidos fins que o **CONTRATO 49/2023,** que tem por objeto o fornecimento de Solução de Segurança NGFW com Subscrição e Produto, incluindo instalação, capacitação técnica, garantia e suporte, visando atender as necessidades da Câmara Municipal de Goiânia, foi celebrado na data de **09/11/2023** e assinado pelos representantes legais da empresa **JRV SERVIÇOS LTDA-ME (XLOGIC SOLUÇÕES EM TI)** e da **CÂMARA MUNICIPAL DE GOIÂNIA.**

KEITE KELLE DE SOUZA PEREIRA
RG: 5828524 SSP/GO
CPF: 758.095.241-68

MIZMAR GONÇALVES DE SOUZA SIMÕES
RG: 5480255 PC-GO
CPF: 022.669.571-98

Documento assinado eletronicamente por:

- **KEITE KELLE DE SOUZA PEREIRA**, **CD - COPAM**, em 09/11/2023 12:09:29.
- **MIZMAR GONCALVES DE SOUZA SIMOES**, **SV - DRGER**, em 09/11/2023 12:10:02.

Este documento foi emitido pelo SUAP em 09/11/2023. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.camaragyn.go.gov.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 74330
Código de Autenticação: 2ee98b4d17

RELATÓRIO

RELATÓRIO 1 - Arquivo de assinatura aprovado

Data de verificação	09/11/2023 14:35:49 UTC
Versão do software	2.11rc5

Informações do arquivo

Nome do arquivo	Contrato_49-2023_-_Firewall_assinado_assinado_assinado (2).pdf
Resumo SHA256 do arquivo	5c41b7b11902a3fed812b0adddb9e52a44f1671dca4de894ac4115678834e39f
Tipo do arquivo	PDF
Quantidade de assinaturas	5

Informações da LPA

- LPA CAdES v2

Informações de política

- PA_AD_RB_v2_3.der (2.16.76.1.7.1.1.2.3)

BR Assinatura por CN=ANTONIO VICENTE BARBOSA DO VALE

BR Assinatura por CN=ANTONIO VICENTE BARBOSA DO VALE

Informações da assinatura

Tipo de assinatura	Destacada
Status da assinatura	Aprovado
Caminho de certificação	Aprovado
Estrutura da assinatura	Conformidade com o padrão (ISO 32000).
Cifra assimétrica	Aprovada
Resumo criptográfico	Correto
Data da assinatura	01/11/2023 13:49:45 UTC
Status dos atributos	Aprovados

- Informações do assinante
- Caminho de certificação
- Atributos

BR Assinatura por CN=RICARDO CARVALHO RIOS

BR Assinatura por CN=VITOR PESSOA LOUREIRO DE MORAIS:***542931**, OU=AC Instituto Fenacon RFB, OU=EM BRANCO, OU=RFB e-CPF A3, OU=Secretaria da Receita Federal do Brasil - RFB, OU=PRESENCIAL, OU=37622727000110, O=ICP-Brasil, C=BR

Informações da assinatura

Tipo de assinatura	Destacada
Status da assinatura	Aprovado
Caminho de certificação	Aprovado
Política utilizada	PA_AD_RB_v2_3.der (2.16.76.1.7.1.1.2.3)
Estrutura da assinatura	Conformidade com o padrão (ISO 32000).
Cifra assimétrica	Aprovada
Resumo criptográfico	Correto
Data da assinatura	09/11/2023 13:31:13 UTC
Status dos atributos	Aprovados