1. OBJETO

1.1. Contratação de renovação de licenciamento de solução de Firewall *Sonicwall*, contemplando todas as funcionalidades já instaladas em cluster de 02 (dois) *Appliances* Modelo NSa3650 com garantia e suporte técnico à solução, e software de gerenciamento e monitoramento *Analytics,* pelo período de 12 meses.

2. JUSTIFICATIVA

2.1. Histórico de Aquisições:

- Em 2019, através do PE 001/2019 (sei 201800029995568), foi adquirido um cluster de firewall SonicWall, modelo NSa3650, licenciado por 3 (três) anos.
- Em junho/2022, foi adquirida a renovação das subscrições da solução (sei 202200029991857) pelo valor de R$ 87.000,00, também licenciado por mais 3 (três) anos.
- Devido a data limite informada pelo fabricante ser até somente agosto/26 , essa última renovação do NSa 3650 será somente de **12 meses.**

2.1.1. *Apliances* da solução instalados na Contratante:

2.1.1.1. FIREWALL SONICWALL NSa3650 CLUSTER 01 - Número de Série : 2CB8ED18B780

2.1.1.2. FIREWALL SONICWALL NSa3650 CLUSTER 02 - Número de Série : 2CB8ED09C080

2.2. Como a garantia finda em Agosto/2025, faz se necessário aquisição de novas subscrições para evitar paralização dos serviços da AGR. Conforme consulta no Fabricante Sonicwall, a data limite de tempo de vida para renovação deste equipamento modelo SonicWall NSa 3650 é até agosto/26, e após essa data em diante não serão mais disponibilizadas atualizações. Sendo assim, a renovação deverá somente de **12 meses.**

2.3. Ao fazer uso ou oferecer serviços por meio da internet ou por outras redes parceiras, a AGR deve ter extrema preocupação com esse canal de comunicação, pois além do incomensurável benefício de permitir conectividade em âmbito global, também representa, em contrapartida, risco potencial para acessos não autorizados e maliciosos. Neste contexto torna-se imprescindível a adoção de soluções que minimizem os riscos e evitem prejuízos, não só em relação às questões que envolvem tecnologia, mas também de ordem financeira e da imagem institucional do órgão.

2.4. É importante frisar que caso ocorra algum ataque malicioso, além da paralisação dos equipamentos instalados, compromete sobremaneira a segurança da informação e a comunicação de dados, possibilitando inclusive, a perda de dados ou o vazamento de informações. Em 2021 o Brasil foi o 5º maior país a sofrer ataques cibernéticos, e, os sites de governos sofreram muitos ataques, como Ministério da Saúde, ConectSUS, Sistema de Informação do Programa Nacional de Imunização, Controladoria Geral da União - CGU , Polícia Rodoviária Federal - PRF. O Brasil viu mais de 95 milhões de ataques de malware nos últimos quatro meses de 2021 (000028913995). Só com ransomwares, foram mais de 33 milhões de ataques ao longo do ano. Foi país com o maior número desses incidentes em toda a América Latina. Em dezembro/2021 e em fevereiro/2022, o Portal de Serviços Eletrônicos da AGR sofreu tentativas de invasão (000028914010), a página ficou fora do ar, porém a base de dados não sofreu violações ou acesso não autorizado.

2.4.1. Em 2024, os ataques cibernéticos aumentaram em todo o mundo, incluindo no Brasil, e se tornaram uma ameaça cada vez maior. O Gabinete de Segurança Institucional do Brasil registrou mais de 8.600 ataques cibernéticos a órgãos públicos brasileiros em 2024, o dobro do ano anterior. O Instituto Nacional de Combate ao Cibercrime (INCC) estima que os ataques cibernéticos podem ter custado R$ 2,3 trilhões à economia brasileira em 2024. A IBM calculou que o custo médio por violação de dados no Brasil em 2024 foi de R$ 6,75 milhões. Em relação aos ataques cibernéticos em 2024 no mundo, o *ransomware* continua a ser uma das principais ameaças à cibersegurança, sequestrando dados de empresas e exigindo resgates milionários. Novas variantes de *ransomware* surgem constantemente, muitas vezes baseadas em códigos vazados na dark web. Um ataque paralisou vários hospitais em Londres, obrigando-os a interromper serviços essenciais e a declarar estado de emergência.

2.5. Perante aos fatos expostos e com o advento de novas ameaças tecnológicas, faz-se necessária a renovação das licenças dos firewalls existentes de forma garantir a continuidade da segurança da rede e dentro da nossa infraestrutura de tecnologia da informação.

2.6. Assim, para aumentar a segurança destes serviços hospedados nos servidores situados na sala de equipamentos da informática, controlar os acessos à internet, proteger contra possíveis tentativas de acesso indevido e disponibilizar uma ferramenta de Acesso Remoto (VPN) para colaboradores, é necessária tal renovação.

2.7. Como forma de proteger o investimento e o conhecimento adquirido para o operação do equipamento existente, recomendado que mantenha a padronização dos equipamentos SonicWall, modelo NSa3650.

2.8. Sendo assim devemos observar que as ações a serem tomadas para resolução dos problemas encontrados com relação à segurança da informação, bem como a elaboração de uma política de prevenção, devem ser realizadas com presteza e procurando as melhores técnicas e equipamentos de implementação, optando-se pela adoção de um projeto que contemple a renovação das licenças e suporte na solução de firewall desta Agência. Esta renovação trará mais segurança à infraestrutura do órgão, zelando pela integridade e guarda das informações.

2.9. Benefícios: Visibilidade e conscientização situacional completa do ambiente de segurança de rede, Análise profunda investigativa e forense, Obter conhecimento e compreensão sobre os riscos e ameaças potenciais reais, Corrigir riscos com maior clareza, certeza e velocidade, Reduzir o tempo de resposta a incidentes em tempo real

2.10. A aquisição está alinhada com o PPA 2024-2027, conforme:

- EIXO ESTRATÉGICO DO PPA: GOIÁS DA GOVERNANÇA E GESTÃO TRANSFORMADORA: tem o intuito reestabelecer a confiança nas instituições, oferecer serviço de qualidade para a sociedade, fomentar o controle social e reconhecer e valorizar o servidor como agente transformador da sociedade.

- OBJETIVO ESTRATÉGICO DO PPA: ATENDIMENTO DE EXCELÊNCIA: Garantir a prestação de serviços públicos com alto nível de excelência, preferencialmente por meio de modernas plataformas digitais.

- ESTRATÉGIAS DO PPA: Adoção de Tecnologias Modernas e melhores práticas que proporcionem aumentar a qualidade do gasto público, tomada de decisão e combate a evasão fiscal;

- DIRETRIZES PLANO DE GOVERNO NO PPA: Políticas de TI centralizadas sendo seguidas e cumpridas pelos órgãos setoriais, norteando o interesse público como referência na execução das atividades tecnológicas

- PROGRAMA: 1048 - GOIÁS DA GESTÃO TRANSFORMADORA

- PRODUTO: MODERNIZAÇÃO DOS SERVIÇOS DA AGR

2.11. A contratação está alinhada ao PDTI 2024-2025 do estado de Goiás: (https://goias.gov.br/governo/plano-diretor-de-tecnologia-da-informacao-pdti/)

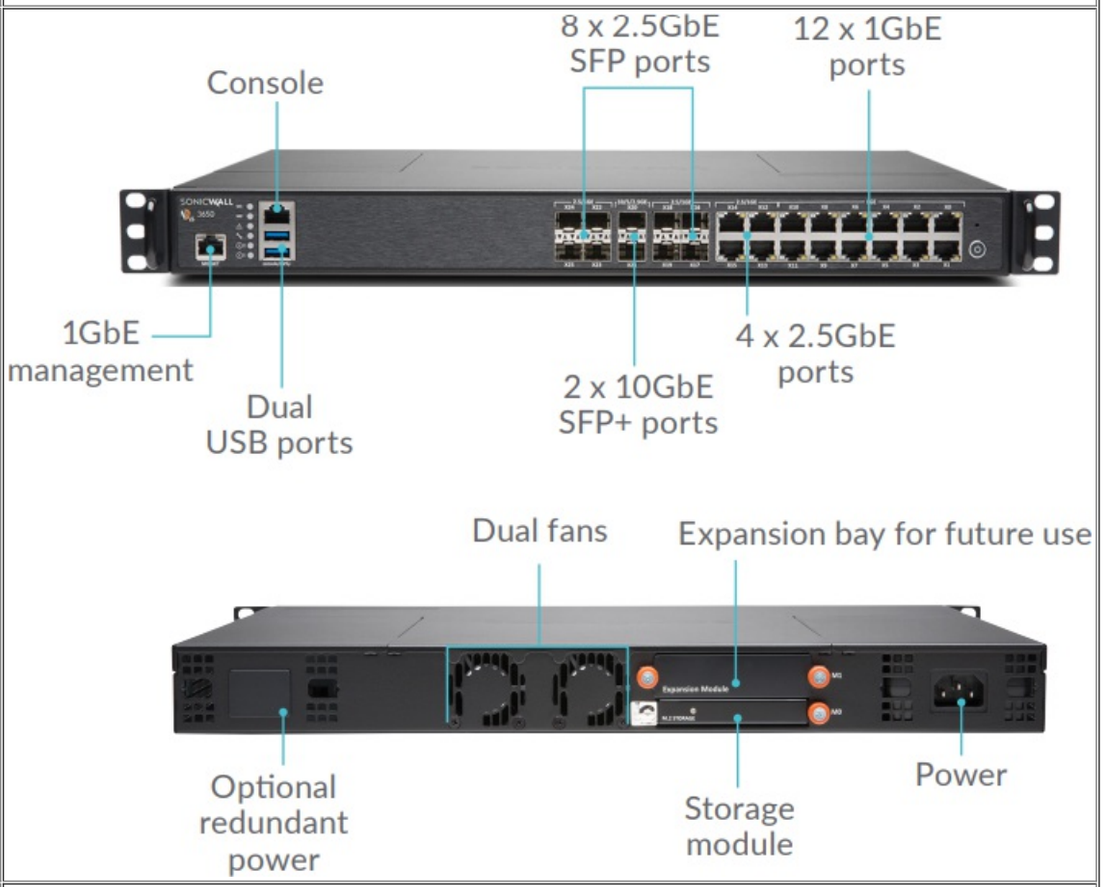
2.11.1. Pilares Estratégicos:

- E1. Potencializar a Transformação Digital no setor público para promover eficiência, transparência e participação cidadã.

- E2. Estabelecer uma estrutura de Governança de Tecnologia da Informação robusta e transparente para reduzir a burocracia e mitigar riscos.
- E3. Estabelecer uma estrutura de Infraestrutura de Tecnologia da Informação segura, eficiente e orientada por dados no setor público.

3. ESPECIFICAÇÕES TÉCNICAS

3.1. Serviço de renovação subscrição de solução de segurança para equipamentos do cluster da marca SonicWall, modelo NS 365, pelo período de 12 meses, conforme especificações discriminadas abaixo:

Funcionalidades	**SonicWall NSa3650.**
Foto	
Part Number	2CB8ED18B780 Primary 2CB8ED09C080 Secundary
Perfomance de Firewall	3.75 Gbps
Firewall and IPS throughput	1.75 Gbps
VPN	1.5 Gbps
IPS	1.8 Gbps

3DES/AES VPN	300 Mbps
Maximum connections	2.000.000 conexões
Quantidade de interfaces	2 x 10-GbE SFP+, 8 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE Management, 1 Console
Datasheet SonicWall Nsa 3650	https://www.sonicwall.com/resources/datasheet/network-security-appliance-nsa-series/

3.2. Disponibilização da Sistema de Gerenciamento e Monitoramento de Segurança (SonicWall Analytics) (sislog 200429 sei 72534934)

3.2.1. Gerenciamento centralizado de segurança e rede - Gerenciamento e monitoramento do ambiente de segurança de rede distribuído.

3.2.2. Configuração de política federada - Definição de políticas do firewall SonicWall, pontos de acesso wireless, segurança de e-mail, dispositivos de acesso remoto seguro e switches de um local central.

3.2.3. Gerenciamento de pedido de mudança e fluxo de trabalho - Garantia da correção e da conformidade das mudanças de políticas, aplicando um processo para configurar, comparar, validar, revisar e aprovar políticas antes da implementação. Os grupos de aprovação podem ser configurados pelo usuário para conformidade com a política de segurança da empresa. Todas as alterações de políticas são registradas em um formato auditável que garante que o firewall esteja em conformidade com os requisitos regulamentares. Todos os detalhes granulares de quaisquer alterações feitas são historicamente preservados para ajudar na conformidade, na auditoria e na solução de problemas.

3.2.4. Implementação Zero-Touch - implementação e o provisionamento remoto de firewall SonicWall remotamente usando a nuvem. Envia políticas automaticamente, executa atualizações de firmware e sincroniza licenças.

3.2.5. Implementação e configuração de VPN sofisticada - gerenciamento de painel único de toda a infraestrutura de segurança da rede.

3.2.6. Gerenciamento off-line - implementação e o provisionamento remoto do firewall SonicWall remotamente usando a nuvem. Envio de políticas automaticamente, executa atualizações de firmware e sincroniza licenças.

3.2.7. Gerenciamento de licenças simplificado - ativação da conectividade VPN e consolidação das políticas de segurança.

3.2.8. Painel universal - widgets personalizáveis, mapas geográficos e relatórios centrados no usuário.

3.2.9. Monitoramento e alerta de dispositivos ativos - alertas em tempo real com recursos integrados de monitoramento e facilitação dos esforços de solução de problemas, permitindo que os administradores tomem medidas preventivas e forneçam correção imediata.

3.2.10. Suporte a SNMP - interceptações eficientes e em tempo real para todos os dispositivos e aplicações de Transmission Control Protocol/Internet Protocol (TCP/IP) e SNMP, aprimoramento de solução de problemas para identificar e responder a eventos críticos da rede.

3.2.11. Visualização e inteligência de aplicações - relatórios históricos e em tempo real de quais aplicações estão sendo usadas e por quais usuários. Relatórios personalizáveis usando recursos intuitivos de filtragem e drilldown.

3.2.12. Opções de integração - interface de programação de aplicações (API) para serviços da Web, suporte à interface de linha de comando (CLI) para a maioria das funções e suporte a interceptações SNMP para provedores de serviços e empresas.

3.2.13. Relatórios HIPAA, PCI e SOX - Inclui modelos de relatórios PCI, HIPAA e SOX predefinidos para satisfazer as auditorias de conformidade de segurança.

3.2.14. Agregação de dados - mecanismo analítico orientado por inteligência automatiza a agregação, a normalização, a correlação e a contextualização dos dados de segurança que passam por todos os firewalls.
3.2.15. Contextualização de dados - A análise acionável, apresentada de forma estruturada, significativa e facilmente consumível, capacita a equipe de segurança, o analista e as partes interessadas a descobrir, interpretar, priorizar, tomar decisões e tomar ações defensivas apropriadas.
3.2.16. Análise de streaming - Streams de dados de segurança de rede continuamente processados, correlacionados e analisados em tempo real e os resultados são ilustrados em um painel visual dinâmico e interativo.
3.2.17. Análise do usuário - Análise detalhada das tendências de atividade dos usuários para obter visibilidade total de sua utilização, acesso e conexões em toda a rede.
3.2.18. Visualização dinâmica em tempo real - Por meio de uma única tela, a equipe de segurança pode realizar análises investigativas drilldown e análises forenses de dados de segurança com maior precisão, clareza e velocidade.
3.2.19. Detecção e correção rápidas - Recursos de investigação para perseguir atividades inseguras e gerenciar e corrigir rapidamente os riscos.
3.2.20. Análise e relatórios de fluxo - agente de relatório de fluxo para análise de tráfego de aplicações e dados de uso por meio de protocolos IPFIX ou NetFlow para monitoramento em tempo real e histórico. Interface eficaz e eficiente para monitorar visualmente sua rede em tempo real, fornecendo a capacidade de identificar aplicações e sites com alta demanda de largura de banda, visualizar o uso da aplicação por usuário e antecipar ataques e ameaças encontrados pela rede. Visões dos relatórios: Visualização em tempo real com personalização de arrastar e soltar; Tela de relatório em tempo real com filtragem de um clique; Painel de controle de fluxo superior com botões de um clique Visualizar por; Tela Relatórios de fluxo com cinco guias adicionais de atributo de fluxo; Tela de Análise de fluxo com eficientes recursos de correlação e giro; Visualização de sessão para *drilldowns* profundos de sessões e pacotes individuais.

3.2.21. Análise de tráfego de aplicações - Insights eficientes do tráfego de aplicações, da utilização de largura de banda e das ameaças de segurança, ao mesmo tempo em que fornece recursos eficientes de solução de problemas e análise forense.

3.3. Funcionalidades do Gerenciamento e Monitoramento

3.3.1. Painel de resumo com visualizações e gráficos

Taxa de largura de banda, Utilização da CPU, Contagem de conexões, Taxa de conexão por segundo, Índice de risco (escala de um a dez), Porcentagem de bloqueio, Total de conexões, Total de dados transferidos, Principais aplicações, Principais intrusões, Principais categorias de URL, Principais vírus, Número de vírus, intrusões, spyware, botnets,

3.3.2. Streaming de monitor em tempo real com gráficos de áreas/barras

Aplicações, Entrada/saída da interface, média, mín., pico, Largura de banda, Taxa de pacotes, Tamanho do pacote, Taxa de conexão; Contagem de conexões; Monitor com múltiplos núcleos.

3.3.3. Principais painéis de resumo com drilldowns

Aplicações, Usuários, Vírus, Intrusões. Spyware, Categorias da Web, Fontes, Destinos, Locais das fontes. Locais dos destinos. Filas de BW, Botnet

3.3.4. Relatórios com drilldowns, exportação para pdf/csv e envio de e-mail agendado:

Aplicações/Usuários/Fontes/Destinos/ Conexões, Total de conexões travadas, Conexões travadas por regra de acesso, Conexões travadas por ameaça, Conexões travadas por filtro de botnet, Conexões travadas por filtro de GeoIP, Conexões travadas por Content, Filtering Service, Vírus, Intrusões, Spyware, Total de dados transferidos, Dados enviados, Dados recebidos, Vírus/Intrusões/Spyware/Categorias da Web/Locais das fontes/Locais dos destinos/Filas de BW, Conexões, Total de dados transferidos, Dados enviados, Dados recebidos, Botnet, Conexões. Exportação .pdf, .csv. Relatórios agendados, Relatório de fluxo, Capture Threat Assessment (SWARM), Diária/Semanal/Mensal, Arquivo/E-mail/PDF.

3.3.5. Visualizador de sessão do Analytics com drilldowns, filtragem, exportação de dados de sessões individuais - Análise de tráfego em qualquer combinação de: Aplicação, Categoria da aplicação, Risco da aplicação, Assinatura, Ação, IP do iniciador/respondente, País do iniciador/respondente, Porta do iniciador/respondente, Bytes do iniciador/respondente, Interface do iniciador/respondente, Índice do iniciador/respondente, Gateway do iniciador/respondente, MAC do iniciador/respondente, Protocolo, Taxa (Kbit/s), ID do fluxo, Intrusão, Vírus, Spyware, Botnet

3.3.6. Análise de ameaças/travamentos em qualquer combinação de Nome da ameaça, Tipo de ameaça, ID da ameaça, Aplicação, Categoria da aplicação, Risco da aplicação, Assinatura, Ação, IP do iniciador/respondente, País do iniciador/respondente, Porta do iniciador/respondente, Bytes do iniciador/respondente, Interface do iniciador/respondente, Índice do iniciador/respondente, Gateway do iniciador/respondente, MAC do iniciador/respondente, Protocolo, Taxa (Kbit/s), ID do fluxo, Intrusão, Vírus, Spyware, Botnet

3.3.7. Análise de URL/travamentos em qualquer combinação de URL, Categoria da URL, Domínio da URL, Aplicação, Categoria da aplicação, Risco da aplicação, Assinatura, Ação, IP do iniciador/respondente, País do iniciador/respondente, Porta do iniciador/respondente, Bytes do iniciador/respondente, Interface do iniciador/respondente, Índice do iniciador/respondente, Gateway do iniciador/respondente, MAC do iniciador/respondente. Protocolo: Taxa (Kbit/s), ID do fluxo, Intrusão, Vírus, Spyware, Botnet

3.3.8. Monitor do fluxo de análise de drilldown e giro nos parâmetros de fluxo. Aplicações: Nomes, Categorias, Assinaturas. Usuários: Nome, Endereço IP, Nomes de domínios, Tipos de autenticação, Atividades da Web, Sites, Categorias da Web, URLs. Fontes: Endereços IP, Interfaces, Países. Destinos: Endereços IP, Interfaces, Países. Ameaças: Intrusões: Vírus, Spyware, Spam, Botnets. VoIP: Tipos de mídia, IDs dos chamadores. Dispositivos: Endereços IP, Interfaces: Nomes. Conteúdo: Endereços de e-mail, Tipos de arquivos. Gerenciamento da largura de banda: Entrada, Saída, Todos, URL, Sessões, Total de pacotes, Total de bytes, Ameaças

3.3.9. Gráficos em estrela visualizações de ponto a ponto, drilldowns e giros de Fontes/Usuários/Locais/Dispositivos: Para/de Destinos, Aplicações, Atividades da Web, Ameaças. Filtrado por: Número de conexões, Dados transferidos, Pacotes trocados, Número de ameaças, Realce com halo para: Ameaças, Dados > 1 MB, Conexões >1000, Pacotes >1000.

4. QUANTIDADE E VALORES ESTIMADOS

4.1. Os valores estimados foram obtidos através de média de 03 orçamentos prévios (sislog 200426) conforme planilha de composição de preços (200428):

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR ESTIMADO MÉDIO UNITÁRIO	VALOR ESTIMADO MÉDIO GLOBAL (12 meses)
1	RENOVAÇÃO de Licenciamento de solução de cluster firewall SonicWall por 12 (doze) meses 01 ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 3650 - 1 ANO 01 SOFTWARE ANALYTICS FOR NSA 3650 - 1 ANO 02 Apliances instalados na Contratante: FIREWALL SONICWALL NSa3650 CLUSTER 01 - Número de Série : 2CB8ED18B780 FIREWALL SONICWALL NSa3650 CLUSTER 02 - Número de	1	R$ 6.347,68	R$ 76.172,12

	Série : 2CB8ED09C080			

5. VIGÊNCIA DO CONTRATO

5.1. O prazo de vigência do contrato será de 12 (doze) meses a contar da data de sua assinatura.

5.2. O prazo de garantia dos produtos contra defeitos de fabricação, sem ônus para a Contratante, será o da garantia ofertada pelo fabricante, contados da data do seu recebimento definitivo, que não poderá ser inferior a 12 (doze) meses.

5.3. A execução da garantia e serviços técnicos por empresas terceirizadas, não exime a contratada das responsabilidades assumidas com o contratante.

5.4. A garantia sobre programas de computador abrange tão somente a existência de defeitos de fabricação na mídia entregue a Contratante , de acordo com o Termo de Garantia emitido pelo fabricante do produto e que com ele deverá seguir em anexo.

6. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

6.1. Entregar o software no prazo máximo de até 20 (vinte) dias corridos, a contar da emissão da Nota de Empenho.

6.2. Entregar o software conforme as especificações técnicas exigidas, acompanhado de nota fiscal discriminando o quantitativo referente às licenças de uso, de acordo com as especificações.

6.3. Fornecer o software original de instalação em mídia, manuais de instalação e operação, assim como do seu uso e todas as suas funcionalidades, e demais documentações originais do fabricante. Toda a documentação fornecida pela empresa deverá ser em português (Brasil) e, no caso da inexistência desta por parte do fabricante do software, será aceita em língua inglesa ou espanhola.

6.4. Prestar todos os esclarecimentos técnicos relativos atendimento de 1º nível pertinentes à instalação das licenças, a mal funcionamento dos equipamentos e atualizações das licenças que lhe forem solicitados pela Contratante, relacionados com as características e funcionamento do software cotado.

6.5. Preservar o domínio, não divulgar nem permitir a divulgação, sob qualquer hipótese, das informações a que venha a ter acesso em decorrência dos serviços realizados, sob pena de responsabilidade civil e/ou criminal.

6.6. Cumprir, às suas próprias expensas, todas as cláusulas contratuais que definam suas obrigações.

6.7. Arcar com todas as despesas, diretas ou indiretas, decorrentes do fornecimento dos softwares, sem qualquer ônus ao Contratante.

6.8. Substituir todo e qualquer produto que for entregue com defeito ou aquele que não satisfaça as especificações exigidas.

6.9. Responder por danos materiais ou físicos, causados por seus empregados ou prepostos, diretamente à Contratante ou a terceiros, decorrentes de sua culpa ou dolo.

6.10. Contratada não poderá subcontratar, ceder ou transferir, total ou parcialmente, o objeto deste Edital.

6.11. A Contratada se compromete a fornecer, em qualquer tempo, todas as informações necessárias a fiel execução do objeto, assim como notificar a Contratante caso ocorra imprevistos. Em caso de imprevistos, a Contratada deverá notificar de imediato a Contratante e informar as devidas medidas que serão tomadas visando à solução dos mesmos.

6.12. Cumprir fielmente o Contrato/Instrumento Equivalente, de modo que no prazo estabelecido, o objeto contratado seja entregue.

6.13. Assumir, ainda, a responsabilidade pelos encargos fiscais, sociais, previdenciários e outros decorrentes da contratação.

6.14. A Contratada se obriga neste termo de referência: instalação lógica, orientações aos usuários finais ou qualquer outro serviço aplicado aos softwares especificados.

6.15. O suporte de 2º nível à Contratante deverá ser dado pelo próprio fabricante do software.

6.16. O suporte a ser contratado não envolverá configurações de políticas de segurança no Firewall.

7. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE.

7.1. Receber o produto, testá-lo e aprová-lo quando atender o objeto contratado.

7.2. Efetuar o pagamento à contratada dentro dos prazos preestabelecidos.

7.3. Notificar a Contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas nos produtos recebidos para que sejam adotadas as medidas corretivas necessárias.

7.4. Acompanhar e fiscalizar a execução do contratado/instrumento equivalente, bem como atestar na nota fiscal/fatura a efetiva entrega dos softwares adquiridos e o seu aceite.

7.5. Aplicar à Contratada as sanções regulamentares e contratuais, garantido o contraditório e a ampla defesa.

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

7.7. Verificar minuciosamente, a conformidade dos produtos recebidos com as especificações constantes do Termo de Referência e da

proposta, para fins de aceitação e recebimento definitivos.

7.8. Notificar o fornecedor, por escrito, sobre imperfeições, falhas ou irregularidades constatadas nos produtos fornecidos, para que sejam corrigidos.

7.9. Realizar configurações de políticas de segurança no Firewall

8. PRAZO E LOCAL PARA PRESTAÇÃO DO SERVIÇO E FORMA DE RECEBIMENTO

8.1. Os softwares deverão ser entregues na GETEC/AGR - Gerência de Tecnologia da AGR, localizada na Avenida Goiás, Número 305, Setor Central, Goiânia - GO, CEP: 74.005-010, no horário das 08h às 12h e das 14h às 18h, sendo o frete, carga e descarga por conta da contratada até o local do recebimento.

8.2. Os softwares serão recebidos por servidor designado pela Contratante para tal fim.

8.3. A contratada deverá comunicar a GETEC/AGR, com 72h de antecedência, a data e o horário previsto para a entrega dos softwares, por escrito e/ou através do telefone (62) 3226-6467.

8.4. O prazo para fornecimento dos softwares, instalação e configuração não poderá ser superior a 20 (vinte) dias corridos, contados a partir do recebimento da nota de empenho.

8.5. Os produtos deverão ser entregues conforme as quantidades totais adjudicadas à licitante, de acordo com o Edital.

8.6. Os objetos deverão ser entregues em embalagem adequada para proteger o conteúdo contra danos durante o transporte, desde a origem até o local da entrega, devendo consignar, obrigatoriamente, as suas validades, quando for o caso.

8.7. A contratante fará a verificação da qualidade, do quantitativo e da conformidade do material às especificações definidas neste Termo.

8.8. No ato de entrega dos produtos, apresentar relação contendo identificação de partes e componentes e demais informações que possam auxiliar o recebimento.

8.9. Entregar, juntamente com o produto ofertado, todos os manuais, instruções de uso, instalação e configuração, originais do fabricante, preferencialmente em português, necessária à instalação e operação dos mesmos.

8.10. A Contratada se reserva o direito de aceitar os softwares com versão superior à proposta oferecida pela empresa vencedora, caso no momento da entrega tenha sido disponibilizada ao mercado versão superior.

8.11. Para os casos de vícios ocultos, o tratamento dar-se-á de acordo com o Código de Defesa do Consumidor, ou seja, nos termos do § 3º do artigo 26, no caso de vício oculto, o prazo decadencial de 30 dias para reclamar junto ao fornecedor inicia-se a partir do momento em que for evidenciado o defeito/imperfeição que torne o material impróprio para utilização/consumo - §6, III, do artigo 18.

8.12. Os produtos serão analisados pela Contratante, sendo devolvidos se estiverem em desacordo com as especificações do edital para substituição pela empresa no prazo máximo de 10 (dez) dias.

8.13. Os produtos devem vir acompanhados de todas as mídias necessárias para sua instalação, reinstalação e operação.

8.14. Todas as licenças fornecidas deverão permitir a instalação do produto em quantidade infinita de vezes, guardada a obediência ao quantitativo de licenças fornecidas.

8.15. O mecanismo de expiração ativa após completados os 12 (doze) meses.

8.16. A empresa deverá fornecer o cartão de registro e/ou licença de uso, contendo todas as chaves, senhas, números de identificação, instalação, reinstalação e operação do produto.

8.17. Os softwares serão recebidos da seguinte forma:

8.17.1. Provisoriamente, no ato de entrega, para efeito de posterior instalação e verificação da sua conformidade com as especificações constantes neste Termo de Referência;

8.17.2. Definitivamente, em no máximo 10 (dez) dias úteis contados a partir do recebimento provisório e após a verificação da qualidade dos softwares e sua consequente aceitação, mediante a emissão do Termo de Recebimento Definitivo assinado pelas partes.

8.17.3. O objeto entregue em desconformidade com o especificado no edital e indicado na proposta será rejeitado parcial ou totalmente, conforme o caso, e a Contratada obrigada a substituí-lo no prazo estipulado pela contratante, contado da data do recebimento de notificação escrita, necessariamente acompanhada do Termo de Recusa de Material, sob pena de incorrer em atraso quanto ao prazo de execução.

8.17.4. A notificação mencionada no subitem anterior interrompe os prazos de recebimento e de pagamento até que a irregularidade seja sanada.

8.17.5. Independentemente do aceite, a Contratada garantirá a qualidade de cada unidade do software fornecido pelo prazo estabelecido na respectiva garantia do fabricante, e estará obrigada a substituir aquele que apresentar defeito no prazo estabelecido pela Contratante.

8.17.6. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do produto, nem a ético profissional pela perfeita execução do objeto, dentro dos limites estabelecidos pela lei.

8.17.7 Serão realizados testes dos softwares após instalação, com simulação de todas as funções oferecidas e/ou exigidas, e somente

após será emitido o Termo de Recebimento Definitivo, declarando a conclusão satisfatória dos serviços e o pleno funcionamento dos softwares, para a efetivação do pagamento.

9. FORMA DE PAGAMENTO

9.1. O pagamento será realizado em até 20 (vinte) dias após a apresentação da fatura na GETEC da AGR, devidamente atestada pela unidade competente.

10. GESTOR DO CONTRATO

10.1. A gestão e acompanhamento da entrega e aceite das licenças serão realizados pelos servidores Luciana Dutra Martins e Helton Nunes Silva.

Luciana Dutra Martins

Gerente de Tecnologia da Informação