TRIBUNAL REGIONAL ELEITORAL DE RORAIMA

CONTRATO Nº 5 / 2021

Contrato:	n/d	**Processo:**		**R. Social: Nome F.:**	**SERVICE IT SECURITY CONS SEG TECNOLOGIA DA INFORMAÇÃO LTDA**
ARP:	TRE/PR (0587587)	**CNPJ:**	12.373.559/0001-46	**Fundamento:**	Lei 8.666/93; 10520/2002; Decreto 7892/2013
Proposta:		**Valor:**	R$ 48.489,00	**Objeto:**	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria
Pregão:	03/2020 (0587585)	**Fiscal:**		**Empenho:**	2021NE000142 (0612541)
TR:	TRE-PR (0587585)	**Prazo:**		**Preposto:**	

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE FAZEM ENTRE SI A UNIÃO POR MEIO DO TRIBUNAL REGIONAL ELEITORAL DE RORAIMA – TRE/RR E A EMPRESA SERVICE IT SECURITY CONS SEG TECNOLOGIA DA INFORMAÇÃO LTDA PARA A PRESTAÇÃO DOS SERVIÇOS DE SOLUÇÃO UNIFICADA DE GESTÃO DE VULNERABILIDADES EM ATIVOS DE TECNOLOGIA DA INFORMAÇÃO E APLICAÇÕES WEB.

A **UNIÃO** por intermédio do **TRIBUNAL REGIONAL ELEITORAL DE RORAIMA (TRE-RR),** inscrito no Cadastro Nacional de Pessoa Jurídica (CNPJ/MF) sob o nº **05.955.085/0001-85**, com sede na Avenida Juscelino Kubitschek, n.º 543, São Pedro, nesta cidade, doravante denominado CONSUMIDOR, representado pelo **Sr. Adriano Nogueira Batista** inscrito no CPF sob o n.º 323.230.262-91, no uso das atribuições conferidas pelo art. 56, XVIII, da Regulamento da Secretaria deste Regional (0541224), doravante denominado **CONTRATANTE**, e, de outro lado, a empresa **SERVICE IT SECURITY CONS SEG TECNOLOGIA DA INFORMAÇÃO LTDA** inscrito(a) no CNPJ/MF sob o n.º 12.373.559/0001-46, sediado(a) na Av. Unisinos, n.º 950, 308 Ed. Pe. Rick - São João Batista - São Leopoldo/RS, doravante designada **CONTRATADA**, neste ato representada pela Srª. **Paula Cristina da Silva Lopes,** portador da Carteira de Identidade n.º 2047693169 SSP-PC/RS, CPF n.º 577.510.050-68, telefone (051) 99336-9352; (41) 3155-8500; e-mail: plopes@service.com.br tendo em vista o que consta no Processo n.º 0002488-72.2019.6.23.8000 e em observância às disposições da Lei n.º 8.666, de 21 de junho de 1993, da Lei n.º 10.520, de 17 de julho de 2002, do Decreto n.º 2.271, de 7 de julho de 1997, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão n.º 03/2020 TRE-PR, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Aquisição de solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte 24x7, visando atender às necessidades deste Tribunal Regional Eleitoral, conforme abaixo:

Lote	Item	Descrição	Quantidade	Valor Unitário	Valor Total
3	7	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por ano de uso.	1	R$ 22.000,00	**R$ 22.000,00**
	8	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para 10 domínios (FQDN), por ano de uso.	1	R$ 17.490,00	**R$ 17.490,00**
	9	Instalação, configuração e treinamento inicial para uso da solução, com período mínimo de 16 horas.	1	R$ 8.999,00	**R$ 8.999,00**
		TOTAL		**R$ 48.489,00**	**R$ 48.489,00**

1.2 A Contratação obedecerá ao estipulado neste contrato, bem como às disposições do instrumento convocatório, que, independentemente de transcrição, fazem parte integrante e complementar deste.

CLÁUSULA SEGUNDA – DAS ESPECIFICAÇÕES TÉCNICAS

2.1 – Características Gerais:

2.1.1 - A solução deve ser capaz de realizar varreduras (*scans*) de vulnerabilidades, avaliação de configuração e conformidade (*baseline* e *compliance*), indícios e padrões de códigos maliciosos conhecidos (*malware*).

2.1.2 - A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) por meio da rede.

2.1.3 - A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT.

2.1.4 - Deve ser capaz de identificar no mínimo 45.000 CVEs (*Common Vulnerabilities and Exposures*).

2.1.5 - A solução deve ter a capacidade de adicionar etiquetas (*tags*) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas.

2.1.6 - Deve atribuir a todas as vulnerabilidades uma severidade baseada no *CVSSv3 score*.

2.1.7 - A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades.

2.1.8 - A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades.

2.1.9 - A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente.

2.1.10 - Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:

2.1.10.1 - Por sistema operacional.

2.1.10.2 - Por um determinado software instalado.

2.1.10.3 - Por Ativos impactados por uma determinada vulnerabilidade.

2.1.11 - A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (*Open Vulnerability Assessment Language*).

2.1.12 - A solução deve fornecer gerenciamento de fluxo de trabalho de correção com base em políticas, incluindo a criação e atribuição automática de registro de problema.

2.1.13 - Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente.

2.1.14 - Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual.

2.1.15 - A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades.

2.1.16 - Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial.

2.1.17 - A solução deve ser capaz de aplicar algoritimos de aprendizagem de máquina (*machine learning*) para analizar pelo menos 120 (cento e vinte) características relacionadas a vulnerabilidades.

2.1.18 - O sistema de pontuação e priorização de vulnerabilidades deve avaliar no minímo as seguintes características:

2.1.18.1 - CVSSv3 *Impact Score;*

2.1.18.2 - Idade da Vulnerabilidade;

2.1.18.3 - Se existe ameaça ou exploit que explore a vulnerabilidade;

2.1.18.4 - Número de produtos afetados pela vulnerabilidade;

2.1.18.5 - Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo.

2.1.19 - Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo.

2.1.20 - Deve possuir uma API para automação de processos e integração com aplicações terceiras.

2.1.21 - A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional.

2.1.22 - A solução deve possuir conectores para, no mínimo, as seguintes plataformas:

a) Amazon Web Service (AWS);

b) Microsoft Azure;

c) Google Cloud Platform;

d) Qualys Assets.

2.1.23 - A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML.

2.1.24 - A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados.

2.1.25 - A solução deve ser licenciada para o uso de no minímo 10 (dez) sensores passivos de rede para realizar o monitoramento em tempo real.

2.1.26 - Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo.

2.1.27 - A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:

a) Bancos de dados;

b) *Hypervisors (no mímino VMWare ESX/ESXi)*;

c) Dispositivos móveis;

d) Dispositivos de rede;

e) *Endpoints*;

f) Aplicações.

2.1.28 - Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente.

2.1.29 - Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real sem a necessidade de um agente.

2.1.30 - A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.

2.1.31 - A solução deve ser baseada em nuvem pública, com scanners próprios localizados em nuvem pública e scanners instalados na infraestrutura do cliente (on-premises).

2.1.32 - A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste edital.

2.1.33 - A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

2.1.34 - A atualização da infraestrutura da solução (servidores, bancos de dados, aplicações, sistemas operacionais e configurações) não devem provocar tempo de parada (downtime) superior a 08 (oito) horas por ano.

2.1.35 - A aquisição dos itens poderá ser composta em relação ao tempo. Por exemplo, para atender 750 ativos, por 3 anos, serão adquiridos 9 pacotes do item 1; para atender 20 FQDNs simultâneos por 3 anos, serão adquiridos 6 pacotes do item 2.

2.1.36 - Configuração de segurança e acesso à gerência da solução:

a) A solução deve suportar autenticação de dois fatores para os usuários;

b) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

c) A solução deve permitir a criação de, no mínimo, 10 contas para gerência e acesso aos relatórios, sem custo adicional.

2.1.37 - Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

2.1.38 - Dos Relatórios:

2.1.38.1 - Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda.

2.1.38.2 - A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes.

2.1.38.3 - Deve suportar a criação de relatórios criptografados (protegidos por senha configurável).

2.1.38.4 - A solução deve suportar o envio automático de relatórios para destinatários específicos.

2.1.38.5 - Deve ser possível definir a frequência na geração dos relatórios para no minímo: Diário, Mensal, Semanal e Anual.

2.1.38.6 - Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos.

2.1.38.7 - A solução deve fornecer relatórios do tipo "*scorecard"* para as partes interessadas da empresa.

2.1.38.8 - A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: tendência de ticket por grupo de ativos, usuários e vulnerabilidades.

2.1.39 - A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas.

2.1.40 - A solução deve possuir relatórios pré configurados com as seguintes informações:

2.1.40.1 - *Hosts* verificados sem credenciais.

2.1.40.2 - *Top* 100 Vulnerabilidades mais critícas.

2.1.40.3 - *Top* 10 *Hosts* infectados por *Malwares*.

2.1.40.4 - *Hosts* exploráveis por *Malwares*.

2.1.40.5 - Total de vulnerabilidades que podem ser exploradas pelo *Metasploit*.

2.1.40.6 - Vulnerabilidades críticas e exploráveis.

2.1.40.7 - Máquinas com vulnerabilidades que podem ser exploradas.

2.1.41 - A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade.

2.1.42 - A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

2.1.43 - A solução proposta deve ser de mesmo fabricante, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console central web unificado, sendo toda infraestrutura de aplicações, bancos de dados de vulnerabilidades, dashboards, agentes e plugins também mantidas pelo mesmo fabricante, oferecida como serviço padrão.

2.1.44 - O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Sigilo e Responsabilidade (conforme anexo IV), em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

2.2 - ITEM 7 – Plataforma de Software para Gestão de Vulnerabilidades

2.2.1 - A plataforma de software deve ser capaz de realizar varreduras (*scans*) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados.

2.2.2 - A plataforma de software deve ser licenciada para no minímo 10 *scanners* (prevendo redundância).

2.2.3 - Deve permitir a configuração de vários painéis e *widgets*.

2.2.4 - Deve ser capaz de medir e reportar ameaças.

2.2.5 - Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado.

2.2.6 - A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como *appliances* virtuais.

2.2.7 - A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.

2.2.8 - A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades.

2.2.9 - A plataforma de software deve permitir o monitoramento por meio de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

2.2.10 - A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia.

2.2.11 - No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser cap az de ser reiniciado de onde parou.

2.2.12 - A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura.

2.2.13 - A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e *Active Directory*) e root para sistemas Linux.

2.2.14 - A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo.

2.2.15 - A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.

2.3 - ITEM 8 – Solução de Análise Dinâmica em Aplicações Web

2.3.1 - A solução de análise deve realizar varreduras de vulnerabilidades em aplicações *Web*, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP *Top* 10, CWE e WASC.

2.3.2 - A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações *Web.*

2.3.3 - A solução de análise deverá ser capaz de executar varreduras em sistemas *Web* por meio de seus endereços IP ou FQDN (DNS).

2.3.4 - Deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação.

2.3.5 - A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal.

2.3.6 - Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

a) *Cookies, Headers*, Formulários e Links;

b) Nomes e valores de parâmetros da aplicação;

c) Elementos JSON e XML;

d) Elementos DOM.

2.3.7 - Deverá também permitir a execução da função *crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação.

2.3.8 - A solução de análise deve suportar a integração com o *software Selenium* para permitir sequências de autenticação complexas.

2.3.9 - A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente.

2.3.10 - Suporte a *Postman Collections* para testes de API REST.

2.3.11 - Suportar *override* de DNS para os testes de aplicações *Web*.

2.3.12 - A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo *Web.*

2.3.13 - Deve ser capaz de utilizar scripts customizados de *crawling* com parâmetros definidos pelo usuário.

2.3.14 - Deve ser capaz de excluir determinadas URLs da varredura por meio de expressões regulares.

2.3.15 - Deve ser capaz de excluir determinados tipos de arquivos por meio de suas extensões.

2.3.16 - Deve ser capaz de instituir no mínimo os seguintes limites:

a) Número máximo de URLs para *crawling* e navegação;

b) Número máximo de diretórios para varreduras;

c) Número máximo de elementos DOM;

d) Tamanho máximo de respostas;

e) Tempo máximo para a varredura;

f) Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação *Web;*

g) Número máximo de requisições HTTP(S) por segundo.

2.3.17 - Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual.

2.3.18 - Deve suportar o envio de noticações por email.

2.3.19 - Deverá ser compatível com avaliação de *web services* REST e SOAP.

2.3.20 - A solução de análise deve suportar os seguintes esquemas de autenticação:

a) Autenticação Básica (*Digest*);

b) NTLM;

c) Autenticação de *Cookies;*

d) Autenticação por meio de *Selenium.*

2.3.21 - Deve ser capaz de importar *scripts* de autenticação *Selenium* previamente configurados pelo usuário.

2.3.22 - Deve ser capaz de customizar parâmetros *Selenium* como: *delay* de exibição da página, *delay* de execução de comandos e *delay* de comandos para recepção de novos comandos.

2.3.23 - A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades.

2.3.24 - Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações.

2.3.25 - Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências.

2.3.26 - Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação.

2.3.27 - Serviço de Detecção de *Malware:*

a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente – Item 1;

b) A solução de análise deve ter a capacidade de varrer e identificar infecções por *malware* nas propriedades da aplicação *web;*

c) A solução de análise deve suportar capacidade de detecção de *malware* de dia zero;

d) A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por *malware;*

e) A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação específica, que serão exportados para os formatos HTML e PDF.

2.3.28 - A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:

a) *WordPress*;

b) *Blog Designer Plugin for Wordpress;*

c) *Event Calendar Plugin for Wordpress;*

d) *Convert Plus Plugin for Wordpress;*

e) *Apache, Apache Tomcat, Apache Tomcat JK connector, Apache Spark, Apache Struts, Lighttpd, Nginx;*

f) *Atlassian Confluence, Atlassian Crowd e Atlassian Jira;*

g) *AngularJS, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Magento, Modernizr, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;*

h) *JBoss EAS* e *WildFly.*

2.4 - ITEM 9 – Instalação e Treinamento

2.4.1 - Efetuar as configurações iniciais, em conjunto com a Contratante, para uso da solução proposta, incluindo criação de *scans*, relatórios, filtros, permissões de usuários e demais funcionalidades da solução.

2.4.2 - Apoio na instalação de scanners e agentes on-premises.

2.4.3 - Promover treinamento à equipe técnica da Contratante para configurar, instalar componentes e operar a solução, com no mínimo 16 (dezesseis) horas e para um mínimo de 8 (oito) participantes, nas dependências da contratante, em idioma Português.

CLÁUSULA TERCEIRA – DO RECEBIMENTO DO OBJETO

3.1 - Do recebimento provisório: será feito no ato da entrega das licenças, pelo servidor devidamente designado, ou seus substitutos, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Contrato.

3.2 - Do recebimento definitivo: será feito pelo mesmo servidor ou seus substitutos, após o treinamento ou entrega do voucher, o que ocorrer primeiro.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA CONTRATADA

4.1 – Da entrega:

4.1.1 – Do prazo de entrega/prestação de serviços:

4.1.1.1 – Para os itens 01 e 02: o fornecimento das licenças de software deverá ocorrer em até 05 (cinco) dias corridos a partir da assinatura do contrato.

4.1.1.2 – Para o item 03: a instalação, configuração, customização, criação de relatórios, filtros, criação de dashboards para gestão e operação, repasse básico para operação deverão ocorrer em até 07 (sete) dias corridos após a assinatura do contrato. O treinamento será agendado conforme disponibilidade das partes, mas em prazo não superior a 90 (noventa) dias da data de assinatura do contrato.

4.1.1.2.1 - Se o treinamento, não for executado em até 07 (sete) dias após a assinatura do contrato, deverá ser emitido um voucher para futura realização do mesmo, obedecendo ao prazo máximo disposto no item acima.

4.1.2 – Do local de entrega: as licenças deverão ser entregues e os serviços prestados no Tribunal Regional Eleitoral de Roraima, no horário compreendido entre 08h e 15h, localizado na Av. Juscelino Kubistchek, n.º 543, São Pedro, Boa Vista - RR, na Coordenadoria de Infraestrutura e Comunicação (CIC).

4.1.2.1 – As entregas e serviços deverão ser agendados previamente pelo telefone (95) 2121-7021, com o Sr. Josenilson Verde Lemos ou o Sr. Severino José Caetano Filho.

4.2 - Do fornecimento das licenças de software:

4.2.1 - Fornecer todas as licenças de software necessárias para utilização completa da solução, pelos períodos adquiridos.

4.2.2 - Registrar, junto aos fabricantes e em nome da contratante, todas as assinaturas de licenças de software ofertadas.

4.3 - Das demais obrigações da contratada:

4.3.1 - Cumprir fielmente as obrigações assumidas, conforme as especificações constante neste Contrato de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos/prestar os serviços, nos prazos indicados.

4.3.2 - Prestar todos os esclarecimentos que forem solicitados pelo TRE-RR, credenciando junto ao órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto.

4.3.3 - Assinar, pelo seu responsável legal, Termo de Sigilo e Responsabilidade, conforme modelo constante no Anexo IV, garantindo o sigilo e a confidencialidade dos dados a que vier a ter contato durante a instalação e durante a utilização da solução de software.

4.3.4 - A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

4.4 - Manter durante toda a execução do contrato, as obrigações assumidas na licitação.

CLÁUSULA QUINTA – DA DESPESA ORÇAMENTÁRIA

5.1 - Os recursos destinados à contratação estão assegurados por meio da nota de empenho - 2021NE000142 (0612541) e classificação abaixo:

PTRES	FONTE	ND	SUBITEM	TÍTULO	PI
167894	127	339040	06	LOCAÇÃO DE SOFTWARES	TIC LOCSOF

CLÁUSULA SEXTA – DA VIGÊNCIA

6.1 – O presente contrato vigorará **até 31.12.2021**, podendo ser rescindido antecipadamente nos termos da Lei nº 8.666/93.

CLÁUSULA SÉTIMA – DO PAGAMENTO

7.1 – Pela execução dos serviços, o Contratante pagará à Contratada**,** o valor total de **R$ 48.489,00** (quarenta e oito mil, quatrocentos e oitenta e nove reais), conforme abaixo:

Lote	Item	Descrição	Quantidade	Valor Unitário	Valor Total
3	7	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por ano de uso.	1	R$ 22.000,00	R$ 22.000,00
	8	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para 10 domínios (FQDN), por ano de uso.	1	R$ 17.490,00	R$ 17.490,00
	9	Instalação, configuração e treinamento inicial para uso da solução, com período mínimo de 16 horas.	1	R$ 8.999,00	R$ 8.999,00

7.1.1 – O pagamento será realizado em etapas, conforme abaixo:

a) Itens 7 e 8 – após o recebimento das licenças;

b) Item 9 – após a realização do treinamento ou entrega do voucher, o que ocorrer primeiro.

7.2 – Do documento fiscal:

7.2.1 – O documento fiscal deverá atender os requisitos abaixo, podendo ser emitido na forma eletrônica (Nota Fiscal Eletrônica - NFe), nos termos da legislação vigente, devendo ser encaminhado ao gestor do contrato do TRE/RR por e-mail, cic@tre-rr.jus.br, em formato PDF; ou emitido na forma física, devendo ser encaminhado à Assessoria de Contratos e-mail: ac@tre-rr.jus.br, localizada na Av. Juscelino Kubistchek, n.º 543, São Pedro, Boa Vista - RR.

7.2.1.1 – O CNPJ cadastrado no sistema Comprasnet/documentos de habilitação, para fins de participação no certame, deverá ser o mesmo para efeito de emissão das notas fiscais/faturas para posterior pagamento.

7.2.1.2 - Caso a CONTRATADA não possa emitir as notas fiscais/faturas com o mesmo CNPJ habilitado, poderá fazê-lo através da eventual matriz ou filial da mesma empresa CONTRATADA. Nesse caso, ambos os CNPJs (CONTRATADA e eventual matriz ou filial utilizada) deverão estar com a documentação fiscal regular e atender obrigatoriamente os seguintes requisitos:

- CNPJ da CONTRATADA

- CNPJ do TRE/RR: 05.955.085/0001-85;

- Data de emissão da nota fiscal;

- Descritivo dos valores mensais,

- Número do contrato;

- Banco; Agência; Número da conta corrente (obrigatoriamente da própria CONTRATADA).

7.2.1.3 - A Nota Fiscal/Fatura, após o atestado do gestor da contratação, será encaminhada à Secretaria de Orçamento, Finanças e Contabilidade, para que se efetive o pagamento.

7.3 – Das condições do pagamento:

7.3.1. - O pagamento somente ocorrerá depois de atestado pelo gestor do contrato designado para esta finalidade. O atestado será realizado, obedecendo o prazo e formulário específico, conforme dispositivos legais deste TRE/RR.

7.3.2 - O pagamento ocorrerá em parcela única e será efetuado mediante crédito em conta corrente, conforme indicação da CONTRATADA no documento fiscal, por intermédio de ordem bancária, no prazo de **até 20 (vinte) dias** corridos a partir do atestado pelo gestor do contrato.

7.3.2.1 – Será considerado como data do pagamento, o dia em que constar como emitida a ordem bancária para pagamento.

7.3.3 – O gestor da contratação do TRE/RR procederá à conferência dos requisitos da nota fiscal/fatura, que deverá estar de acordo com as descrições contidas na nota de empenho, bem como apresentar o mesmo número de CNPJ cadastrado, habilitado e constante nos documentos entregues, não se admitindo notas fiscais/faturas emitidas com outro CNPJ, salvo na hipótese prevista no item 7.2.1.2.

7.3.3.1 – Havendo erro na apresentação do documento fiscal ou dos documentos pertinentes à contratação, ou ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará pendente até que a CONTRATADA providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação, não acarretando qualquer ônus para o TRE/PR.

7.3.4 – O TRE/RR, observados os princípios do contraditório e da ampla defesa, poderá deduzir, do montante a pagar à CONTRATADA, acréscimos decorrentes de mora no recolhimento de tributos/contribuições, bem como de multa decorrente de previsão deste contrato.

7.3.5 - Na eventual ocorrência de atraso de pagamento, e desde que a CONTRATADA não tenha concorrido para tanto, serão devidos encargos moratórios pelo TRE/RR, entre a data prevista para o pagamento e a do efetivo pagamento, mediante solicitação formal do interessado, que serão calculados por meio da aplicação da seguinte fórmula: EM = I x N x VP

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso;

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = i/365 (onde i = taxa percentual anual no valor de 6%)

I = (6/100)/365

7.4 – Da regularidade fiscal:

7.4.1 – Todo e qualquer pagamento, decorrente da presente contratação, será precedido de verificação, por parte do TRE/RR, da regularidade fiscal da CONTRATADA em vigor na data do pagamento.

7.4.1.1 – A CONTRATADA inadimplente quanto à regularidade fiscal estará sujeita à abertura de processo administrativo pelo Gestor da contratação do TRE/PR, visando à regularização.

7.4.1.1.1 – Permanecendo a inadimplência poderá haver rescisão contratual, independentemente da aplicação das sanções previstas neste contrato.

7.4.2 – A regularidade de que trata o subitem anterior poderá ser verificada:

a) por meio de consulta on-line no Sistema de Cadastramento Unificado de Fornecedores - SICAF e/ou;

b) por meio de consulta aos sites oficiais e/ou;

c) por meio da apresentação de documentação, pela CONTRATADA, anexada ao documento fiscal.

7.4.2.1 – O resultado das consultas, de que trata as alíneas acima, serão realizadas pelo setor financeiro responsável e deverão constar do processo de pagamento.

CLÁUSULA OITAVA – DA SUBSTITUIÇÃO TRIBUTÁRIA

8.1 – Da substituição tributária:

8.1.1 - Serão feitas as retenções tributárias federais e municipais incidentes sobre a contratação, conforme artigo 64 da Lei 9.430/96, IN RFB 1234/12, IN RFB 971/09, LC 116/2003 e LC 123/06, conforme o objeto da contratação.

8.2 – Dos tributos federais:

8.2.1 - Será efetuada a retenção dos tributos federais aplicando-se, sobre o valor a ser pago, o percentual constante da Tabela de Retenção da IN RFB 1234/12.

8.2.2 - Quando a empresa for optante do Regime Simplificado Nacional (SIMPLES), não haverá a retenção de que trata o item acima.

8.2.3 - A nota fiscal, cuja empresa contratada seja Optante do SIMPLES, deverá estar acompanhada da Declaração, nos termos do caput do artigo 6º da IN RFB 1234/12 - anexo IV.

8.3 - Da retenção previdenciária:

8.3.1 - Quando o objeto da contratação contemplar cessão de mão de obra ou empreitada, poderá ocorrer a retenção do INSS prevista no artigo 112, sobre os serviços elencados nos artigos 117 e 118 da IN RFB 971/09.

8.4 - Da retenção do ISS:

8.4.1 - Sobre serviços, poderá ocorrer a retenção do ISS, quando o objeto da contratação se enquadrar no inciso II, do § 2º do art.6º da LC 116/03.

8.4.2 - Quando a empresa for optante do Regime Simplificado Nacional (SIMPLES), deverá destacar na nota fiscal de prestação de serviços a alíquota na qual está enquadrada, conforme os anexos III ou IV da Lei Complementar 123/06. Caso não haja o referido destaque, será considerada a alíquota máxima vigente, ou seja, 5% (cinco por cento).

8.5 - Quanto à incidência das retenções de tributos prevalecerá sempre a legislação vigente, mesmo que venham a contrariar as disposições acima, conforme sua incidência ou não sobre o objeto contratado.

CLÁUSULA NONA – DO REAJUSTE

9.1 – O reajuste dos contratos com vigência até 01 (um) ano encontra-se suspenso até disciplinamento diverso, oriundo de legislação federal e nas condições.

CLÁUSULA DÉCIMA – DO GESTOR DO CONTRATO

10.1 – A fiscalização e gestão da presente contratação serão realizadas por servidores formalmente designados para este fim.

10.2 – Nos termos da Lei nº 8.666/93, art. 67, parágrafos 1º e 2º, caberá aos Gestores:

a) Receber e atestar o documento fiscal referente à aquisição, encaminhando-o ao setor responsável da Secretaria de Orçamento, Finanças e Contabilidade do TRE/PR para pagamento;

b) Acompanhar o fornecimento de acordo com as condições do edital, determinando o que for necessário para regularização das faltas ou defeitos observados, sob pena de responsabilização administrativa.

c) Comunicar à CONTRATADA, via e-mail, carta ou ofício, defeitos ou irregularidades encontradas na execução do objeto, fixando prazos para solução dos problemas identificações e correções.

d) Se a inexecução persistir, o Gestor deverá criar um Processo Administrativo Digital (PAD) específico de abertura de processo administrativo e encaminhá-lo à Secretaria de Gestão Administrativa, devidamente instruído com todas as informações pertinentes, por meio de formulário específico, anexando-se cópia do comunicado referido no subitem anterior, referente à intenção de abertura de processo administrativo, com o respectivo comprovante de recebimento pela licitante.

CLÁUSULA DÉCIMA PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS

11.1 – O descumprimento de quaisquer das obrigações descritas no presente instrumento poderá ensejar abertura de processo administrativo, garantido o contraditório e a ampla defesa, com aplicação das seguintes sanções, de acordo com o capítulo IV da Lei nº 8666/93:

a) Advertência: faltas leves, de menor gravidade, que não acarretarem prejuízo na prestação dos serviços.

b) Multas:

b.1. De 1% (um por cento) ao dia, até o limite máximo de 15% (quinze por cento), sobre o valor total do respectivo item, a cada ocorrência de atraso injustificado nos prazos de:

a) Entrega das licenças (itens 1 e 2);

b) Início e/ou conclusão dos treinamentos (item 3);

c) Início, atendimento e/ou conclusão da manutenção/chamado do suporte;

d) Substituição do objeto recusado ou com vícios;

b.1.1. Após o 15º (décimo quinto) dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como não executado.

b.2. De 20% (vinte por cento) sobre o valor total do respectivo item a cada ocorrência de:

a) Recusa injustificada em executar o respectivo item, desde que configure inexecução parcial;

b) Entrega parcial das licenças (itens 1 e 2)

c) Execução parcial do treinamento (item 3);

d) Execução parcial da instalação e configuração (item 3);

e) Não substituição de objeto recusado ou com vícios, desde que configure inexecução parcial;

f) Outras hipóteses de inexecução parcial.

b.3. De 25% (vinte e cinco por cento) sobre o valor total do item adjudicado, nos casos de:

a) Recusa injustificada em executar o respectivo item, desde que configure inexecução total;

b) Recusa injustificada em iniciar a entrega das licenças (itens 1 e 2);

c) Recusa injustificada em iniciar a instalação/treinamento (item 3);

d) Não substituição de objeto recusado ou com vícios, desde que configure inexecução total;

e) Outras hipóteses de inexecução total do objeto.

b.4. De 30% (trinta por cento) sobre o valor total do item adjudicado no caso de descumprimento do Termo de Sigilo e Responsabilidade.

b.5. As multas são autônomas e a aplicação de uma não exclui a outra, desde que motivadas por fatos diversos.

c) Impedimento de licitar e contratar com a União, conforme previsto no art. 7º da Lei nº 10.520/02, bem como o descredenciamento do SICAF, ou dos sistemas de cadastramento de fornecedores a que se refere o inciso XIV, do art. 4º, da Lei nº 10.520/02, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, conforme a gravidade do inadimplemento da obrigação, quando a empresa, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.

11.2 - As multas imputadas à CONTRATADA, cujo montante seja superior ao mínimo estabelecido pelo Ministério da Fazenda e não pagas no prazo concedido pela Administração, serão inscritas em Dívida Ativa da União e cobradas com base na Lei nº 6.830/80, sem prejuízo da correção monetária.

11.3 - A CONTRATADA autoriza desde já ao desconto de multa pré-determinada em processo administrativo que garanta a ampla defesa, na primeira fatura a que vier fazer jus. Artigo 1.º, inciso I da Portaria n.º 75 do Ministério da Fazenda, publicada em 22/03/2012.

CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO DO CONTRATO

12.1 - Ficará o presente contrato rescindido, a juízo da administração, mediante formalização, assegurado o contraditório e a defesa, nos casos elencados no art. 78 a 80 da Lei 8.666/93.

CLÁUSULA DÉCIMA TERCEIRA – DOS CASOS OMISSOS

13.1 - Os casos omissos serão decididos pelo Contratante, segundo as disposições contidas na Lei 8.666/93 e, subsidiariamente, na Lei 9.784/99, no Código de Defesa do Consumidor e demais normas e princípios gerais aplicáveis.

13.2 - Será também causa de rescisão se a Contratada alocar funcionários, para o desempenho dos serviços, que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento de membros ou juízes vinculados a este Tribunal, contrariando o artigo 3º da Resolução nº 07, de 18/10/2005, com redação dada pela Resolução nº 09, de 06/12/05, ambas do CNJ (Conselho Nacional de Justiça).

CLÁUSULA DÉCIMA QUARTA – DO FORO

14.1 - Fica eleito o Foro de Boa Vista - RR, com expressa renúncia de qualquer outro, por mais privilegiado que possa vir a ser, para dirimir eventuais divergências oriundas do presente contrato.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

Boa Vista, 14 de abril de 2021.

Adriano Nogueira Batista
Diretor-Geral
(documento assinado eletronicamente)

Paula Cristina da Silva Lopes
Representante legal da CONTRATADA

Documento assinado eletronicamente por **Paula Cristina da Silva Lopes**, **Usuário Externo**, em 14/04/2021, às 13:45, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ADRIANO NOGUEIRA BATISTA**, **Diretor-Geral**, em 14/04/2021, às 15:14, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rr.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0611934** e o código CRC **54B651E7**.