ANEXO I

TERMO DE REFERÊNCIA

1 – OBJETO

1.1 - Registro de Preços para aquisição de s**olução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte 24x7**, de acordo com as especificações e condições descritas neste Termo de Referência.

2 – DAS ESPECIFICAÇÕES E CARACTERÍSTICAS

2.1 - Poderão ser contratados os itens abaixo, agrupados em LOTES, conforme quantitativos, características e especificações a seguir:

LOTE	Item	Código SIASG	DESCRIÇÃO	Quantidade			Valor Máximo aceitável Unitário (R$)
				TRE/PR	TRE/SP	TRE/RR	
1	1	27502	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.	09			51.538,03
	2	27502	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para 10 domínios (FQDN), por ano de uso.	06			41.200,33
	3	20052	Instalação, configuração e treinamento inicial para uso da solução, com período mínimo de 16 horas	01			11.500,00
2	4	27502	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. (Desmembrado do 1 – Local de entrega)		03		51.538,03
	5	27502	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para 10 domínios (FQDN), por ano de uso. (Desmembrado do 2 – Local de entrega)		03		41.200,33
	6	20052	Instalação, configuração e treinamento inicial para uso da solução, com período mínimo de 16 horas. (Desmembrado do 3 – Local de entrega)		01		11.500,00
3	7	27502	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. (Desmembrado do 1 – Local de entrega)			01	51.538,03
	8	27502	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para 10 domínios (FQDN), por ano de uso. (Desmembrado do 2 – Local de entrega)			01	41.200,33
	9	20052	Instalação, configuração e treinamento inicial para uso da solução, com período mínimo de 16 horas. (Desmembrado do 3 – Local de entrega)			01	11.500,00

2.1.1 – Os itens abaixo referem-se exatamente ao mesmo objeto. Foram desdobrados em itens distintos devido ao local de entrega ser diferente:

a) **1, 4 e 7;**
b) **2, 5 e 8;**
c) **3, 6 e 9.**

2.2 – Características Gerais:

2.2.1 - 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*).

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

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

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

2.2.5 - 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.

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

2.2.7 - 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.

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

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

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

2.2.10.1 - Por sistema operacional.

2.2.10.2 - Por um determinado software instalado.

2.2.10.3 - Por Ativos impactados por uma determinada vulnerabilidade.

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

2.2.12 - 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.

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

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

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

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

2.2.17 - 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.

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

2.2.18.1 - CVSSv3 *Impact Score;*

2.2.18.2 - Idade da Vulnerabilidade;

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

2.2.18.4 - Número de produtos afetados pela vulnerabilidade;

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

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

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

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

2.2.22 - 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.

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

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

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

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

2.2.27 - 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.

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

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

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

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

2.2.32 - 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.

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

2.2.34 - 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.

2.2.35 - 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.

2.2.36 - 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.

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

2.2.38 - Dos Relatórios:

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

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

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

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

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

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

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

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

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

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

2.2.40.1 - *Hosts* verificados sem credenciais.

2.2.40.2 - *Top* 100 Vulnerabilidades mais critícas.

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

2.2.40.4 - *Hosts* exploráveis por *Malwares*.

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

2.2.40.6 - Vulnerabilidades críticas e exploráveis.

2.2.40.7 - Máquinas com vulnerabilidades que podem ser exploradas.

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

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

2.2.43 - A solução proposta nos lotes 01, 02 e 03 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.

2.2.44 - 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.

2.3 - ITEM 1, 4 e 7 – Plataforma de Software para Gestão de Vulnerabilidades

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

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

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

2.3.4 - Deve ser capaz de medir e reportar ameaças.

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

2.3.6 - 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.

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

2.3.8 - 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.

2.3.9 - 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.

2.3.10 - 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.

2.3.11 - 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.

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

2.3.13 - 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.

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

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

2.4 - ITEM 2, 5 e 8 – Solução de Análise Dinâmica em Aplicações Web

2.4.1 - 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.

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

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

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

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

2.4.6 - 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.

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

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

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

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

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

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

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

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

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

2.4.16 - 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.

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

2.4.18 - Deve suportar o envio de noticações por email.

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

2.4.20 - 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.*

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

2.4.22 - 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.

2.4.23 - 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.

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

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

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

2.4.27 - Serviço de Detecção de *Malware:*

a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente – Item 1, 4 e 7;

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.

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

a) *WordPess;*
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.*

2.5 - ITEM 3, 6 e 9 – Instalação e Treinamento

2.5.1 - 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.

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

2.5.3 - 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.

3 - DAS OBRIGAÇÕES DA CONTRATADA

3.1 – Da entrega:

3.1.1 – Do prazo de entrega/prestação de serviços:

3.1.1.1 – 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.

3.1.1.2 – 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.

3.1.1.2.1 - 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.

3.1.2 – Do local de entrega:

3.1.2.1 – Tribunal Regional Eleitoral do Paraná: as licenças deverão ser entregues e os serviços prestados no Tribunal Regional Eleitoral do Paraná, no horário compreendido entre 12h e 19h, localizado na rua João Parolin, 224, Prado Velho, Curitiba – PR.

3.1.2.1.1 – As entregas e serviços deverão ser agendados previamente pelo telefone (41) 3330-8614, com o Sr. Zilmar de Souza Junior ou o Sr. Juarez de Oliveira.

3.1.2.2 – Tribunal Regional Eleitoral de São Paulo (órgão participante): as entregas serão realizadas na sede do Tribunal Regional Eleitoral de São Paulo, rua Francisca Miquelina, nº 123, São Paulo/SP, CEP 13.160-000.

3.1.2.3 – Tribunal Regional Eleitoral de Roraima (órgão participante): as entregas serão realizadas na sede do Tribunal Regional Eleitoral de Roraima, avenida Getúlio Vargas, nº 225, Bairro São Pedro, Boa Vista/RR, CEP 69.306-050.

3.2 - Do fornecimento das licenças de software:

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

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

3.3 - Das demais obrigações da contratada:

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

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

3.3.3 - 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.

3.3.4 - 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 - DEVERES E RESPONSBILIDADES DO ÓRGÃO CONTRATANTE

4.1 – Receber o objeto conforme abaixo:

4.1.1 – Tribunal Regional Eleitoral do Paraná:

4.1.1.1 - Do recebimento provisório: será feito no ato da entrega das licenças, pelo servidor Zilmar de Souza Junior (SIDS), ou seus substitutos, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência.

4.1.1.2 - Do recebimento definitivo: será feito pelo servidor Zilmar de Souza Junior (SIDS), ou seus substitutos, após o treinamento ou entrega do voucher, o que ocorrer primeiro.

4.1.2 – Tribunal Regional Eleitoral de São Paulo e Tribunal Regional Eleitoral de Roraima (órgãos participantes): o recebimento será efetuado em conformidade com as orientações destes órgãos.

4.2 - Devolver o objeto em desacordo com as especificações exigidas no edital.

4.3 - Cumprir todos os compromissos financeiros assumidos com a Contratada no prazo estipulado.

4.4 - Proporcionar todas as facilidades, inclusive esclarecimentos atinentes ao objeto, para que a empresa possa cumprir as obrigações dentro das normas e condições da aquisição.

4.5 - Promover, por meio de seu representante, o acompanhamento e a fiscalização do objeto contratado, sob os aspectos qualitativos e quantitativos, prazos de vigência e entregas, anotando em registro próprio as falhas detectadas e comunicando ao órgão por escrito as advertências e as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte desta.

5 - DISPOSIÇÕES GERAIS

5.1 - As licitantes deverão efetuar suas cotações seguindo rigorosamente as especificações solicitadas, abstendo-se de participar da licitação aqueles que não puderem atender às condições do edital.

5.2 – Esclarecimento de dúvidas:

5.2.1 – Tribunal Regional Eleitoral do Paraná: Dúvidas referentes à contratação poderão ser sanadas com o servidor Marcelo Charan, pelo telefone: (41) 3330-8621 ou 3339-8681, das 12:00 horas às 19:00 horas.

5.2.2 – Tribunal Regional Eleitoral de São Paulo (órgão participante): para eventuais esclarecimentos de dúvidas ou agendamento de entrega, os licitantes poderão contatar a servidora Silvana Sales Scardini em São Paulo/SP pelo e-

mail silvana.scardini@tre-sp.gov.br ou pelo telefone (11) 3130-2175.

5.2.3 – Tribunal Regional Eleitoral de Roraima (órgão participante): para eventuais esclarecimentos de dúvidas ou agendamento de entrega, os licitantes poderão contatar a servidora Cassia Cavalcante Alves em Roraima/RR pelo e-mail cassia@tre-rr.jus.br ou pelo telefone (95) 2121-7017.