ILUSTRE SENHOR(A) PREGOEIRO(A) DA COMISSÃO PERMANENTE DE COMPRAS E LICITAÇÃO - CPCL.

PREGÃO ELETRÔNICO Nº 024/2020/CPCL/DPE/RO
EDITAL Nº 033/2020/CPCL/DPE/RO

A WEBSECURE CONSULTORIA E SEGURANCA EM TI, inscrita no CNPJ n.º **20.548.658/0001-40**, com endereço na ***RUA BOM FUTURO - JARDIM ALVORADA - ALTO PARAISO - RO***, vem respeitosamente à presença de Vossa Senhoria, com fundamento **item 5**, do Edital do Pregão Eletrônico n.º 024/2020/CPCL/DPE/RO, no prazo legal, apresentar:

SOLICITAÇÃO DE ESLARECIMENTO AO EDITAL DE LICITAÇÃO

pelos motivos de fato e razões de direito abaixo expostas.

I. – TEMPESTIVIDADE.

1. Inicialmente destaca-se que a presente Impugnação é **tempestiva**, uma vez que **o prazo para Solicitação de Esclarecimentos aos termos do Edital de Licitação pelo licitante é até 03 (dois) dias úteis que anteceder a abertura da licitação em sessão pública**, a qual está marcada para o dia **11/12/2020**, às 09h00 (horário de Brasília/DF).

2. Consequentemente, o prazo para impugnar o Edital em questão é até o dia **08/12/2020**.

II. – MÉRITO.

3. Da análise dos autos do Processo Administrativo Eletrônico n.º 024/2020/CPCL/DPE/RO e do Edital de Licitação n.º 033/2020/CPCL/DPE/RO vê-se que existem pontos dúbios que podem levar à uma má interpretação do mesmo, devendo estas ser sanadas antes da realização do certame, conforme exposto abaixo.

1. – ESCLARECIMENTO SOBRE:

Solução de controle de tráfego e segurança (NGFW)

1.1- Segundo o subitem “3.2.” da JUSTIFICATIVA

“No cenário atual, é crescente a demanda pela disponibilização online de serviços com alta disponibilidade, confiabilidade e tolerância a falhas. Nesse ambiente de missão crítica, são necessários mecanismos que melhorem a eficiência dessa infraestrutura, reduzindo custos e simplificando o gerenciamento destes ativos. Estes mecanismos aprimoram a operação da infraestrutura, reduzindo o tempo de interrupção e consequentemente melhorando os níveis de serviço", do item 3.2.”

Entendemos que a **Solução NGFW** deverá ser ofertada em uma “**única unidade”**, conforme informado no **Item 3 da tabela de Espedificações**, mesmo a justificativa dissertando sobre alta disponibilidade. ***Está correto o nosso entendimento?***

Caso estejamos equivocados, solicitamos informar quais as respectivas quantidades para os papéis e funcionalidades ora requisitados.

1.2- Conforme subitem “3.8.3”.

“Camada 3 (l3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação. Gerar roteamento virtual para pelo menos 120 roteadores virtuais e administração do tráfego entre diferentes áreas de segurança e sub-redes, suportando pelo menos 30 áreas de segurança e um mínimo de 120 sistemas virtuais;"

Do item "**Solução de controle de tráfego e segurança (NGFW)**",entendemos que os roteadores virtuais não são integrados ao Firewall, e sim uma particularidade da rede do Cliente, assim o Firewall irá administrar essas redes advindas desses roteadores, sendo responsável pela segurança do tráfego das áreas de Segurança e das redes dos Sistemas Virtuais. ***Está correto o nosso entendimento?***

Caso estejamos equivocados, solicitamos informar se a solução ofertada deva suportar para ativação em aquisição futura pelo menos 120 sistemas virtuais. ***Está correto o nosso 2º entendimento?***

1.3- Conforme subitens "3.20.5.""3.20.6."

"**3.20.5.** Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: *pdf, tar, zip, rar, seven-z, exe, rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm;*"
"**3.20.6**. Deve fazer o bloqueio efetivo do malware desconhecido (Dia Zero) oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente."

Do item "**Solução de controle de tráfego e segurança (NGFW)"**, entendemos que para o pleno atendimento deste item, existem requisitos que devem ser obrigatoriamente ser atendidos, pois os arquivos com suas respectivas extensões, serão descarregados das conexões do NGFW os quais serão totalmente enviados para o ambiente de sandbox podendo ser inloco na DPE-RO ou no site do fabricante, lembrando que caso algum arquivo seja malicioso, para haver o bloqueio sem que o mesmo seja entregue parcialmente ao cliente, todas as conexões que dependerem de inspeção sandbox, ficarão em estado de ""on hold/idle"" na tabela de estado do NGFW até que o ambiente de sandbox envie o veredito para o NGFW, onde caso contadores de sessão sejam excedidos, as respectivas conexões que originaram os respectivos, por terem que inspecionar totalmente antes de entregar ao cliente, serão finalizadas sem a passagem do arquivo retornando ao mesmos mensagens de erros comum de conectividade. Em busca de maior assertividade e oferta que atenda efetivamente em ambiente de produção, composto por diversas conexões e arquivos, para o pleno atendimento deste item, entendemos que:

Torna-se **desejável e não obrigatório** a inspeção total antes de entrega ao cliente, permitindo desta forma a entrega parcial ou ação similar. ***Está correto o nosso entendimento?***

Caso negativo, para formação de proposta e valores, solicitamos informar:

a. **Para o ambiente HTTP:**

I. Qual a quantidade de usuários que utilizarão a funcionalidade;
II. Qual o throughput de tráfego HTTP, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;
III. Tamanho máximo de arquivos a serem enviados a inspeção,
iv. qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

b. Para o ambiente HTTPS:

I. Qual a quantidade de usuários que utilizarão a funcionalidade;
II. Qual o throughput de tráfego HTTPS, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;
III. tamanho máximo de arquivos a serem enviados a inspeção;
IV. Qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

c. **Para o ambiente SMTP via MTA:**

I. Qual a quantidade de usuários que utilizarão a funcionalidade;
II. Qual o throughput de tráfego SMTP, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;
III. tamanho máximo de arquivos a serem enviados a inspeção;
IV. Qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

d. Para o ambiente SMTPS (tls) via MTA:

I. Qual a quantidade de usuários que utilizarão a funcionalidade;
II. Qual o throughput de tráfego SMTPS, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;
III. Tamanho máximo de arquivos a serem enviados a inspeção;
IV. Qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

e. Qual o ttl de sessão máximo permitido no NGFW que fará o hold das sessões até o pleno processamento dos arquivos em sandbox.

f. Caso ocorra erros de inspenção em sandbox, para conexões oriundas de comunicações HTTP e HTTPS, será permitido o envio de mensagens de erro aos navegadores dos clientes?

g. Caso ocorra erros de inspenção em sandbox, para conexões oriundas de comunicações SMTP e SMTPS(TLS), qual o período máximo permitido para o pleno processamento em sandbox?

1.4- Conforme subitem "3.20.9."

"A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;"

Do item "**Solução de controle de tráfego e segurança (NGFW)**", entendemos que solução ofertada deva suportar sistemas operacionais Windows e arquivos Office. ***Está correto o nosso entendimento?***

Caso negativo, para o correto dimensionamento e formação de proposta, ***favor informar os respectivos throughputs de inspeção para cada tipo de versão Windows e Office***.

1.5- Conforme subitem "3.20.10."

"Esse sistema automático de análise "***In Cloud" ou local deve prover***:" do item "**Solução de controle de tráfego e segurança (NGFW)**", entendemos que para a solução ofertada contemplando análise "***In Cloud***", todos os requisitos relacionados a sandbox ***tornam-se desejáveis e não obrigatórios*** por necessitar de comunicação direta com o ambiente de sandbox do fabricante. ***Está correto o nosso entendimento?***

1.6- Conforme subitem "3.20.10.9."

"O sistema de detecção de Malware moderno deve possuir SLA de até 1 hora para finalização da análise e definição de resultado do arquivo analisado." do item "**Solução de controle de tráfego e segurança (NGFW)**",

entendemos que este requisito ***torna-se desejável e não requerido*** devido os diversos fatores que entram colisão com a funcionalidade de sandbox ora requisitadas neste certame. ***Está correto o nosso entendimento?***

Caso contrário favor informar qual a banda e condições de saúde de link de internet que serão garantidos até o data center do fabricante que hospedará o ambiente de sandbox para análise e definição de resultado.

1.7- Conforme subitem "3.25.11."

"Deverá contar com um software cliente de VPN-SSL para os sistemas operacionais Windows SP, Vista (32 e 64 bits), Windows 7 (32 e 64 bits) e Windows 10 (32 e 64 bits)."" do item ""**Solução de controle de tráfego e segurança (NGFW)**", entendemos que *os requisitos de sistemas operacionais pré Windows 7 tornam-se desejáveis e não obrigatórios devido descontinuidade de suporte pela própria Microsoft*. **Está correto o nosso entendimento?**

Caso negativo entendemos que a **DPE-RO assumirá o risco do suporte conforme site da Microsoft na seguinte url** *https://support.microsoft.com/pt-br/windows/o-suporte-ao-windows-xp-terminou-47b944b8-f4d3-82f2-9acc-21c79ee6ef5e*, **assumindo assim a responsabilidade** de todas as funcionalidades que se relacionarem, **eximindo assim a licitante** de obrigações editalícias e contratuais. ***Está correto o nosso entendimento?***

1.8- Conforme subitem "3.27.21."

"Permitir a integração e avaliação de todos os equipamentos de proteção de rede na gerência com os seguintes padrões regulatórios: ***ISO 27001, ISO 27002 e GDPR (base da norma LGPD)***;"

Do item "**Solução de controle de tráfego e segurança (NGFW)**" entendemos que estes requisitos podem ser atendidos por outras metodologias ou normas de segurança mundialmente reconhecidas. Está correto o nosso entendimento?

Caso negativo, **sendo este um Órgão zelador das Leis**, sendo uma delas até **citada acima a "LGPD"**, favor informar

as obrigatoriedades de requisitos que devam ser atendidas segundo as respectivas normas ora requisitadas.

1.9- Conforme subitem "3.27.1."

Caso a solução possua licenças relacionadas a capacidade de log e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;", entendemos serão aceitas soluções com capacidade do Tipo VM (VMware ou Nutanix) onde a quantidade de Log estará restrita à capacidade de Hardware que o Cliente disponibilizará para este fim. ***Está correto o nosso entendimento?***

Caso contrário favor informar qual a capacidade de Hardware será disponibilizará para este fim.

III. – REQUERIMENTOS.

2. Em face do exposto, requer sejam **as presentes SOLICITAÇÕES julgadas procedentes**, com efeito de que sejam **respondidos os esclarecimentos solicitados**, para bem resguardar a efetiva e melhor prestação dos serviços à Administração Pública. Como evidenciado abaixo:

Do princípio da competição ou ampliação da disputa

O princípio da competição relaciona-se à competitividade, **às cláusulas assecuratórias da igualdade de condições a todos os concorrentes**. Viés deste princípio na área econômica é o princípio da livre concorrência *(inciso IV do art. 170 da Constituição Federal).* ***Assim, como a lei reprime o abuso do poder econômico que vise à denominação dos mercados e a eliminação da concorrência, a lei e os demais atos normativos não podem limitar a competitividade na licitação***.

O inciso do § 1º, do art. 3º, da Lei nº 8.666/93 ***ressalta ser vedado aos agentes públicos admitir, prever, incluir ou tolerar, nos atos de convocação, cláusulas ou condições que comprometam, restrinjam ou frustrem o seu caráter competitivo,*** inclusive nos casos de sociedades cooperativas, e ***estabeleçam preferências ou distinções*** em razão da naturalidade, da sede ou domicílio dos licitantes ***ou de qualquer outra circunstância impertinente ou irrelevante para o específico objeto do contrato***. O inciso II do mesmo parágrafo possui resquício dessa vedação ante a proibição de se estabelecer tratamento diferenciado de natureza comercial, legal, trabalhista, previdenciária ou qualquer outra entre empresas brasileiras e estrangeiras.

Qualquer cláusula que favoreça, limite, exclua, prejudique ou de qualquer modo fira a impessoalidade exigida do gestor público poderá recair sobre a questão da restrição de competição.

Conforme o Tribunal de Contas, não se admite a discriminação arbitrária na seleção do contratante, sendo insuprível o tratamento uniforme para situações uniformes, ***tendo em vista que a licitação se destina a garantir não só a seleção da proposta mais vantajosa para a Administração, como também a observância do princípio constitucional da isonomia***. **Acórdão 1631/2007 Plenário (Sumário).**

3. Caso não sejam adotadas as providências necessárias até a data marcada para realização da **Sessão de Abertura** da presente licitação (**11/12/2020**, às 09h00 (horário de Brasília/DF)), a mesma **deverá ser suspensa/cancelada** até que sejam esclarecidos os pontos solicitados.

Termos em que,
Pede e Espera Deferimento.

Alto Paraíso-RO, 08 de dezembro de 2.020.

WEBSECURE CONSULTORIA E SEGURANCA EM TI
CNPJ n.º 20.548.658/0001-40