

Campinas, 03 de janeiro de 2018.

Of. 19.172/2018 – O.E.

Assunto: Esclarecimento 01. Pregão Presencial nº NLP-017/2017

Prezados Senhores,

Em resposta aos pedidos de esclarecimentos, os quais nos foram remetidos por meio de correio eletrônico, conforme descrito abaixo, o Comitê Brasileiro de Clubes - CBC, por intermédio de seu Pregoeiro, vem esclarecer o que segue:

**PERGUNTA:** 1) "5.1.4: - Fazemos Controle de Aplicações, mas não temos WAF no nosso NGFW. Sugestão: retirar este item.

*"A solução deverá ser provida com 2 (dois) equipamentos por localidade, do tipo appliance, com função de firewall de aplicação (WAF – Web Application Firewall), para serem instalados em rack padrão 19."*

**RESPOSTA:** Sugestão não acatada, o objeto pretendido deverá oferecer as funções descritas no edital.

**PERGUNTA:** 2) "5.1.6: - Nossa solução provê tolerância a falhas tanto no modo ativo-ativo quanto no modo ativo-passivo assim como a grande maioria dos demais fabricantes, mas sugerimos que a exigência seja pelo modo ativo-ativo, pois desta forma além de prover a redundância e contingência a falhas, os equipamentos trabalharam em balanceamento de carga aumentando em muito a performance do acesso. No modo ativo-passivo, um equipamento estará funcionando enquanto o outro estará apenas em modo de espera (Stand-by), sendo que o seu custo não justifica este modo de funcionamento.

Sugestão: Alterar para modo de tolerância a falhas ativo-ativo somente.

*"Implementar alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo."*

**RESPOSTA:** Sugestão não acatada, o objeto pretendido deverá oferecer as funções descritas no edital.

**PERGUNTA:** 3) "5.2.17.21: - Suportamos todos os métodos de autenticação padrão de mercado, mas não suportamos Kerberos.

Kerberos é um protocolo de autenticação criado pelo MIT (Massachusetts Institute of Technology), para solucionar problemas de autenticação internos, mas não é um padrão da indústria, ou seja, sua atualização depende do MIT, sendo que se este parar de atualizá-lo, todos que os utilizam ficarão sem suporte.

<https://web.mit.edu/kerberos/>

Sugestão: Alterar para um método de autenticação padrão de mercado como o IEE 802.1x (Radius, LDAP, AD, etc.).

*"Deverá suportar autenticação Kerberos."*

**RESPOSTA:** A autenticação via protocolo Kerberos é uma opção que pode ser oferecida pelo proponente.

No item 5.2.30 existem informações de outros protocolos de autenticação que são aceitos para esse objeto.

**PERGUNTA:** 4) "5.2.18.14: Não suportamos esta feature.

Sugestão: retirar este item.

*"Deverá suportar referência cruzada com CVE (Common Vulnerabilities and Exposures)."*

**RESPOSTA:** Sugestão não acatada, o objeto pretendido deverá oferecer as funções descritas no edital.

**PERGUNTA:** 5) "5.2.19.14: - Na nossa solução de Controle de URL não fazemos atualização manual, temos a feature do Local CFS Responder que funciona de forma diferente porém faz atualização de forma automática onde nossa base de conhecimento de URL fica On-Premise no cliente.

Importante ressaltar que nas nossas soluções as atualizações são feitas de forma automática justamente para que não fiquem vulneráveis a milhares de novas ameaças que surgem a cada hora.

Sugestão: Alterar para um método de atualização apenas automática ou retirar este item.

*"5.2.19.14 A atualização da base de dados deve ser automática com a opção de ser feita manualmente via TFTP."*

**RESPOSTA:** Sugestão não acatada, o objeto pretendido deverá oferecer as funções descritas no edital.

**PERGUNTA:** 6) "5.2.23.1.5: - Suportamos todos os métodos de autenticação padrão de mercado, mas não suportamos Kerberos.

Kerberos é um protocolo de autenticação criado pelo MIT (Massachusetts Institute of Technology), para solucionar problemas de autenticação internos, mas não é um padrão da indústria, ou seja, sua atualização depende do MIT, sendo que se este parar de atualiza-lo, todos que os utilizam ficaram sem suporte.

<https://web.mit.edu/kerberos/>

Sugestão: Alterar para um método de autenticação padrão de mercado como o IEE 802.1x (Radius, LDAP, AD, etc.).

*"Deverá suportar autenticação Kerberos."*

**RESPOSTA:** A autenticação via protocolo Kerberos é uma opção que pode ser oferecida pelo proponente.

No item 5.2.30 existem informações de outros protocolos de autenticação que são aceitos para esse objeto.

**PERGUNTA:** 7) "5.2.27.3: Não suportamos esta feature.

Sugestão: retirar este item.

*"Suporte a roteadores virtuais (Virtual Routers)"*

**RESPOSTA:** Sugestão não acatada, o objeto pretendido deverá oferecer as funções descritas no edital.

**PERGUNTA:** 8) "5.2.30.2.4: - Suportamos todos os métodos de autenticação padrão de mercado, mas não suportamos Kerberos.

Kerberos é um protocolo de autenticação criado pelo MIT ([Massachusetts Institute of Technology](https://web.mit.edu/kerberos/)), para solucionar problemas de autenticação internos, mas não é um padrão da indústria, ou seja, sua atualização depende do MIT, sendo que se este parar de atualiza-lo, todos que os utilizam ficaram sem suporte.

<https://web.mit.edu/kerberos/>

Sugestão: Alterar para um método de autenticação padrão de mercado como o IEE 802.1x (Radius, LDAP, AD, etc.).

*"Deverá suportar autenticação Kerberos."*

**RESPOSTA:** A autenticação via protocolo Kerberos é uma opção que pode ser oferecida pelo proponente.

No item 5.2.30 existem informações de outros protocolos de autenticação que são aceitos para esse objeto.





Nada mais havendo a tratar, informamos que continuamos à disposição para quaisquer outros esclarecimentos no prazo regulamentar.

Em atenção aos princípios constitucionais da publicidade e da isonomia, a presente resposta será encaminhada a todos os interessados que retiraram o edital citado, bem como publicada no sítio eletrônico do CBC.

Atenciosamente,



Delvair Rodrigues Trindade  
Pregoeiro e Presidente da Comissão de Contratação.