Em resposta ao pedido de esclarecimentos da empresa GMX2 Tecnologia, com o apoio da Unidade Técnica do Tribunal, informamos o seguinte:

1. Item 7.1.10.20.3.2

O item exige suporte a objetos dinâmicos com listas externas envolvendo IPs, domínios, URLs, FQDN e Data Centers, incluindo SDDC e SDN.

Solicitamos confirmar se a Administração aceita mecanismos equivalentes, tais como:

- resolução dinâmica de FQDN

- objetos atualizáveis automaticamente,

- uso de APIs para atualização de listas externas, que atendem à finalidade operacional do requisito sem impor arquitetura proprietária.

Resposta: Não será aceito.

2. Itens 7.1.10.20.3.2.1, 7.1.12.4.1 e 7.1.12.4.2

Os itens determinam integração nativa e simultânea com AWS, Azure, Google Cloud, OpenStack, Cisco ACI, VMware NSX-T, vCenter e Kubernetes, além da sincronização automática de objetos para uso em políticas.

Considerando que diversas soluções utilizam APIs padronizadas, automação, orquestração e webhooks que entregam a mesma finalidade, questionamos:

A Administração aceita integração funcional equivalente, desde que:

- permita comunicação via API REST,

- permita obtenção dinâmica de objetos,

- permita atualização automatizada das políticas, garantindo a mesma efetividade do requisito?

Resposta: não será aceito.

3. Itens 7.1.10.20.12 e 7.1.10.22.29

Há exigência de suporte a SAML para autenticação em bases de identidade externas.

Solicitamos confirmar se são aceitos outros protocolos amplamente utilizados, tais como:

- OAuth 2.0,

- OpenID Connect,

- RADIUS/LDAP para SSO,

que cumprem a mesma finalidade de federação e autenticação corporativa.

Resposta: Outros protocolos serão aceitos, mas deverá suportar pelo menos SAML para essa finalidade. Ou seja, o protocolo SAML deverá ser suportado.

4. Item 7.1.10.21.11

O texto estabelece que a solução deve monitorar integridade de aplicações SaaS e realizar decisões baseadas em experiência do usuário, com failover automático para caminhos de melhor desempenho.

Sabendo que esse processo é implementado de forma distinta entre fabricantes, solicitamos confirmar se são aceitos mecanismos equivalentes, tais como:

- medição de jitter, perda e latência por aplicação,

- path selection por métricas de rede,

- failover automático por degradação,

- health-check customizado de URLs SaaS.

Resposta: Não será aceito.

5. Item 7.1.12.10.9

O item exige exportação de logs exclusivamente nos formatos CEF 1.0 ou 0.1.

Como diversos SIEMs operam também com formatos como Syslog RFC5424, JSON estruturado, LEEF, ou conectores via API, solicitamos esclarecer se o objetivo é apenas garantir compatibilidade com SIEM, e se a Administração aceita:

- logs Syslog padronizados,

- exportação via JSON,

- integração via API,

- conversão via conector do próprio SIEM.

Resposta: Deverá suportar, pelos menos, formatos CEF (Common Event Format), versão 1.0 ou 0.1 e CSV conforme os itens 7.1.12.10.9 e 7.1.12.10.10;

Era o que tínhamos a esclarecer.

Goiânia, 10 de dezembro de 2025.

Benedito da Costa Veloso Filho
Agente de Contratação/Pregoeiro