codiub

Licitações Codiub <licitacao@codiub.com.br>

PEDIDOS DE ESCLARECIMENTO - Pregão Eletrônico nº 01/2026

Comercial Security Data <comercial@securitydata.tec.br> 18 de setembro de 2026 às 18:35
Para: licitacao <licitacao@codiub.com.br>

O presente instrumento tem como objetivo precípuo salvaguardar a estrita observância aos princípios constitucionais e infraconstitucionais da isonomia, da impessoalidade, da moralidade, da igualdade e da ampla competitividade que regem as contratações públicas, conforme expressamente positivados no art. 5º e no art. 11 da Lei Federal nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos). As indagações e interpretações técnicas aqui delineadas não buscam, em hipótese alguma, afastar os padrões mínimos de segurança, disponibilidade e integridade almejados pela Administração Pública, mas sim garantir que tais finalidades sejam atingidas mediante a aceitação de soluções de alto padrão tecnológico existentes no mercado corporativo global, evitando-se que escolhas de nomenclatura ou detalhes proprietários de arquitetura restrinjam indevidamente a disputa.

Cumpre destacar que a indicação de marca, modelo ou a adoção de especificações que, por seu excessivo detalhamento, conduzam à exclusividade fática de determinado fornecedor é medida de caráter estritamente excepcional no ordenamento jurídico pátrio, restrita às estritas hipóteses autorizadas pelo art. 41 da Lei nº 14.133/2021 e sempre dependente de robusta e prévia justificativa técnica encartada nos autos do processo administrativo. **Dessa forma, requer-se a confirmação formal de que os requisitos técnicos contidos no Item 5 do Termo de Referência (subitens 5.1 a 5.5.65.4) consubstanciam parâmetros funcionais e níveis de serviço mínimos, e não barreiras restritivas voltadas a inviabilizar a participação de soluções tecnológicas equivalentes.**

II. PARTE I — ITENS 01 E 02 (FIREWALLS CORPORATIVOS DE PRÓXIMA GERAÇÃO) — SUBITENS 5.1 E 5.2

1. Constatação Preliminar — Indícios de Direcionamento Técnico para a Linha de Produtos Fortinet

Da análise técnica e comparativa detalhada realizada entre as exigências constantes do Item 01 (subitem 5.2.1) e do Item 02 (subitem 5.2.2) do Termo de Referência e as especificações públicas disponibilizadas pelos fabricantes de segurança de redes, verificou-se uma coincidência numérica milimétrica e inequívoca entre a totalidade dos parâmetros de desempenho e a composição física de interfaces exigidas e os datasheets comerciais dos equipamentos FortiGate 400G (Item 01) e FortiGate 30G (Item 02), da fabricante Fortinet. Para o Item 01, o instrumento convocatório requisita exatamente 145 Gbps de throughput de firewall, 55 Gbps de VPN IPSec, 25 Gbps de IPS, capacidade para 50.000 túneis simultâneos de clientes VPN IPSec, além de uma exata e singular composição de portas que conjuga interfaces SFP28 25GbE, SFP+ 10GbE, SFP 1GbE, 5GbE RJ45, porta dedicada de Alta Disponibilidade (HA) em 2,5GbE e porta de gerência em chassi 1U com fonte redundante. Para o Item 02, replicam-se exatamente os 3,9 Gbps de firewall, 600.000 conexões simultâneas, 30.000 novas conexões por segundo, 3,5 Gbps de VPN IPSec, 800 Mbps de IPS e 4 portas GbE RJ45.

A identidade integral, cumulativa e simultânea de múltiplos parâmetros de desempenho e de engenharia de hardware com os catálogos de um único fabricante supera qualquer hipótese de convergência fortuita de mercado, evidenciando a transposição literal de especificações proprietárias. Tal conduta afronta diretamente o disposto no art. 9º, inciso III, e no art. 25 da Lei nº 14.133/2021, que vedam categoricamente a inserção de condições que comprometam, restrinjam ou frustrem o caráter competitivo da licitação, bem como o art. 41 do mesmo diploma legal. Diante disso, solicita-se que a Administração esclareça se tais parâmetros foram consolidados com base em ampla pesquisa de mercado e confirme que serão aceitas propostas baseadas em equipamentos de fabricantes líderes de mercado que entreguem desempenho funcional equivalente ou superior, ainda

que com variações de engenharia de hardware e composição de interfaces. **Está correto nosso entendimento?**

2. Sistemas Virtuais e Contextos Lógicos (Subitens 5.1.1.6, 5.1.2.9, 5.1.2.10 e 5.2.1.15)

Entendemos que a finalidade técnica de segregação administrativa, controle de acesso e isolamento de tráfego exigida nos subitens em referência será plenamente atendida por soluções que utilizem mecanismos nativos equivalentes de particionamento e governança, tais como zonas de segurança dedicadas, perfis de administração com escopo de controle restrito e políticas de segurança segregadas por unidade organizacional ou departamento, ainda que a plataforma não adote a nomenclatura comercial ou o conceito arquitetural estrito de "sistemas virtuais" (VDOMs). **Está correto nosso entendimento?**

3. Roteamento Multicast em Modo Denso (Subitem 5.1.2.3)

Entendemos que o objetivo do requisito é garantir a capacidade de distribuição eficiente de tráfego multicast na infraestrutura corporativa, sendo considerada atendida a exigência mediante o suporte comprovado ao protocolo PIM Sparse Mode (PIM-SM), padrão amplamente consolidado e recomendado para redes corporativas modernas, ainda que a solução não disponha do protocolo PIM Dense Mode (PIM-DM).**Está correto nosso entendimento?**

4. Suporte a Mecanismos de Tradução IPv4/IPv6 — NAT46 (Subitem 5.1.2.6)

Entendemos que a finalidade da especificação é garantir a plena interoperabilidade e a transição e convivência entre os protocolos IPv4 e IPv6, sendo aceita a solução que implemente mecanismos consolidados de coexistência, tais como NAT64, DNS64 e NAT66, ainda que não disponibilize especificamente a função de tradução de IPv4 para IPv6 (NAT46). **Está correto nosso entendimento?**

5. Protocolo de Virtualização de Rede VXLAN (Subitem 5.1.2.11)

Entendemos que a finalidade técnica de segmentação lógica, isolamento e interoperabilidade com infraestruturas virtuais e de data center será considerada plenamente atendida por soluções que empreguem mecanismos avançados de VLANs (IEEE 802.1Q), sub-interfaces e zonas de segurança isoladas, bem como suporte nativo a túneis de transporte da própria plataforma, assegurando o perfeito isolamento do tráfego corporativo.

Está correto nosso entendimento?

6. Monitoramento via Protocolo SNMP (Subitem 5.1.2.13)

Entendemos que será considerada plenamente atendida a exigência caso a solução forneça monitoramento contínuo dos seus recursos operacionais (como uso de CPU, memória, interfaces e tráfego) por meio do protocolo padrão SNMP (v2c/v3), complementando a visibilidade de segurança, status de túneis VPN e estado de alta disponibilidade através de sua console centralizada e logs estruturados, ainda que determinados parâmetros de segurança não sejam expostos via OIDs de MIBs proprietárias de SNMP. **Está correto nosso entendimento?**

7. Transporte Seguro de Logs via SSL/TLS (Subitem 5.1.2.15)

Entendemos que a exigência de encaminhamento seguro de logs é integralmente satisfeita pelo suporte a mecanismos modernos de transporte criptografado baseados na suíte de protocolos TLS (Transport Layer Security), sendo indiferente o emprego terminológico de "SSL", denominação historicamente utilizada para referenciar conexões seguras de rede. **Está correto nosso entendimento?**

8. Suporte a OSPF Graceful Restart (Subitem 5.1.2.19)

Entendemos que a finalidade do subitem é assegurar a continuidade do encaminhamento de pacotes e minimizar o impacto de convergência nas tabelas de roteamento durante manobras operacionais ou failover do equipamento, sendo plenamente aceita solução que implemente suporte completo a OSPFv2 e OSPFv3 conjugado a mecanismos próprios de alta disponibilidade com sincronização de estados de sessão e transição transparente de links, ainda que não contenha a configuração proprietária nomeada "OSPF Graceful Restart". **Está correto nosso entendimento?**

9. Licenciamento e Operação em Alta Disponibilidade (Subitem 5.1.2.25)

Considerando que o Termo de Referência prevê a operação dos equipamentos em regime de Alta Disponibilidade (HA), entendemos que a solução ofertada deverá assegurar o arranjo em modo Ativo-Passivo de tal forma que, em caso de falha do equipamento primário, o equipamento secundário assuma de maneira contínua, automática e integral todas as funcionalidades de segurança contratadas (IPS, inspeção SSL/TLS profunda, antivírus de gateway, controle de aplicações e proteção contra ameaças avançadas) sem a exigência de aquisição de licenças adicionais de software ou custos adicionais para a CONTRATANTE. **Está correto nosso entendimento?**

10. Integração com Nuvens Privadas e Orquestradores (Subitem 5.1.2.28)

Entendemos que a finalidade de resguardar a infraestrutura e os fluxos de dados entre ambientes corporativos é atendida mediante a aplicação rigorosa de políticas de segurança de próxima geração, inspeção profunda de pacotes e controle de acesso executados na borda da rede pelos appliances, sendo considerada válida a proposta ainda que a solução não possua conectores de API dedicados e pré-configurados para orquestradores específicos como VMware ESXi, Cisco ACI ou Kubernetes. **Está correto nosso entendimento?**

11. Notificação de Alertas via Plataformas de Mensageria (Subitem 5.1.2.29)

Entendemos que a finalidade do requisito é assegurar a comunicação tempestiva e eficaz de incidentes críticos aos administradores de rede, sendo o subitem atendido mediante o envio de alertas por e-mail (SMTP seguro), traps SNMP e/ou integração via Webhooks customizados, ainda que a solução não disponha de um conector nativo de fábrica rotulado especificamente para Microsoft Teams. **Está correto nosso entendimento?**

12. Controle de Tráfego por Código de País — GeoIP (Subitem 5.1.2.35)

Entendemos que o requisito visa permitir a aplicação de políticas restritivas ou permissivas com base na localização geográfica dos endereços IP (GeoIP), sendo considerada atendida a exigência desde que a solução possibilite o bloqueio ou a liberação de fluxos direcionados a países ou regiões geográficas específicas, independentemente da sintaxe exata ou do padrão de codificação adotado na interface gráfica. **Está correto nosso entendimento?**

13. Base de Reconhecimento de Aplicações em Camada 7 (Subitens 5.1.3.3 e 5.1.11.11)

Entendemos que a exigência técnica visa assegurar uma abrangente visibilidade e governança sobre as aplicações em trânsito na rede corporativa, sendo aceita a comprovação de catálogo de reconhecimento de aplicações com volume igual ou superior a 3.000 aplicações corporativas ativas, mediante apresentação de link da documentação oficial do fabricante, reconhecendo-se a natureza dinâmica e expansiva desse banco de aplicações reconhecidas. **Está correto nosso entendimento?**

14. Assinaturas Personalizadas de Aplicações (Subitem 5.1.3.15)

Entendemos que a necessidade de controle e visibilidade de aplicações proprietárias ou internas da organização será considerada satisfeita pela criação de regras e políticas baseadas em objetos de rede, portas lógicas, serviços customizados e definições de padrões de tráfego, ainda que a interface não disponibilize um editor específico para construção de assinaturas customizadas em camada 7. **Está correto nosso entendimento?**

15. Alertas e Notificações ao Usuário Final (Subitem 5.1.3.17)

Entendemos que o envio de página de bloqueio e conscientização ao usuário final aplica-se ao tráfego baseado no protocolo HTTP/HTTPS via navegador web, enquanto para aplicações de rede não baseadas em navegador o evento será registrado nos logs administrativos do sistema para auditoria, sem exibição de tela de bloqueio ao usuário final. **Está correto nosso entendimento?**

16. Granularidade de Captura de Pacotes em Eventos de IPS (Subitem 5.1.4.28)

Entendemos que a exigência voltada à análise forense e validação de incidentes de segurança será atendida quando a solução disponibilizar mecanismos de captura de pacotes (PCAP) associados aos eventos e assinaturas de IPS conforme as capacidades e parâmetros disponibilizados nativamente na console do fabricante. **Está correto nosso entendimento?**

17. Quantitativo de Categorias de Filtragem Web (Subitem 5.1.5.7)

Entendemos que a finalidade de controle e auditoria do acesso à web será plenamente satisfeita mediante a disponibilização de uma base de filtragem e categorização de URLs atualizada continuamente pela inteligência de ameaças do fabricante, cuja cobertura temática seja igual ou superior a 80 categorias consolidadas de navegação. **Está correto nosso entendimento?**

18. Compatibilidade com Diretório Microsoft Active Directory (Subitem 5.1.6.3)

Entendemos que a integração com a base de usuários é assegurada pela compatibilidade com os protocolos de autenticação padrão de mercado (Kerberos, NTLM e LDAP/LDAPS) suportados pelas versões ativas e homologadas do Microsoft Active Directory, sendo aceita a solução ainda que a documentação vigente não faça menção expressa a sistemas descontinuados pelo fornecedor (como Windows Server 2012 R2). **Está correto nosso entendimento?**

19. Identificação e políticas sobre arquivos criptografados (subitem 5.1.7.3)

O subitem 5.1.7.3 exige a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses arquivos, no âmbito das funcionalidades de filtro de dados (item 5.1.7).

Esclarecemos nosso entendimento nos seguintes termos: a inspeção SSL/TLS, prevista nos subitens 5.1.2.36 e 5.1.2.37, refere-se à decriptografia do túnel de comunicação (transporte HTTPS), permitindo à solução inspecionar o tráfego em texto claro — inclusive os arquivos que trafegam dentro da conexão sem criptografia própria. Já o subitem 5.1.7.3 trata de arquivos criptografados em si (por exemplo, protegidos por senha ou por criptografia no próprio arquivo), cuja inspeção do conteúdo interno depende da respectiva chave de decriptação, indisponível ao equipamento de borda.

Considerando que a inspeção do conteúdo de arquivos criptografados sem a posse da chave constitui limitação técnica comum a todos os fabricantes de mercado, entendemos que o requisito será considerado atendido quando a solução identificar o arquivo criptografado — inclusive quando sua extensão for renomeada, na forma do subitem 5.1.2.38 — e aplicar sobre ele as políticas de segurança configuradas (permitir, bloquear ou registrar), sendo essa capacidade complementada pela inspeção SSL/TLS já prevista nos subitens 5.1.2.36 e 5.1.2.37 para o tráfego em claro. **Está correto nosso entendimento?**

20. Criptografia Legada em Túneis VPN IPSec (Subitens 5.1.9.3 e 5.1.9.4)

Entendemos que a menção a algoritmos criptográficos historicamente depreciados (tais como 3DES, DES, MD5 e SHA-1) tem o exclusivo propósito de viabilizar a eventual interoperabilidade com ativos legados, não constituindo exigência mandatória de uso corporativo, o qual deve priorizar cifras modernas e robustas (famílias AES-GCM/CBC e SHA-256/384/512). **Está correto nosso entendimento?**

21. Interoperabilidade Padronizada de VPN IPSec (Subitem 5.1.9.9)

Entendemos que a capacidade de interoperabilidade da solução com gateways de segurança de terceiros é comprovada pela plena aderência aos padrões abertos da IETF para o protocolo IPSec (IKEv1, IKEv2, ESP e AH), sendo prescindível a homologação nominal ou menção explícita a marcas comerciais específicas na documentação do fabricante. **Está correto nosso entendimento?**

22. Suporte a Clientes de VPN em Ambientes Linux (Subitem 5.1.9.21)

Entendemos que o acesso remoto seguro para estações e servidores com sistema operacional Linux será garantido mediante a compatibilidade com clientes nativos do sistema operacional ou softwares de código aberto homologados para conexões VPN IPSec/SSL, ainda que não haja software cliente de marca proprietária empacotado para todas as distribuições e versões nominais listadas no TR. **Está correto nosso entendimento?**

23. Priorização em tempo real de protocolos de voz (VoIP) (Subitem 5.1.10.10)

O subitem 5.1.10.10 exige suporte à priorização em tempo real de protocolos de voz (VoIP), tais como H.323, SIP, SCCP e MGCP, e aplicações como Skype.

Entendemos que a finalidade do requisito é assegurar a qualidade de serviço (QoS) das comunicações de voz sobre a rede corporativa, garantindo baixa latência, baixo jitter, perda mínima de pacotes e encaminhamento preferencial do tráfego de voz em relação ao tráfego de dados. Nesse sentido, entendemos que essa finalidade será considerada atendida quando a solução permitir a classificação e a priorização do tráfego de voz pelos protocolos padrão de mercado (SIP e H.323), que já dispõem de tratamento otimizado na inspeção de tráfego, bem como a identificação e o controle de aplicações de comunicação (a exemplo de Skype), mediante mecanismos de QoS com filas de prioridade configuráveis e marcação de pacotes (DSCP/802.1p), ainda que não mantenha tratamento nominal dedicado para a totalidade dos protocolos listados, especialmente aqueles legados, proprietários ou em desuso no mercado (SCCP e MGCP). **Está correto nosso entendimento?**

24. Ajuste de Políticas de Balanceamento de Carga (Subitem 5.1.11.5)

Entendemos que o gerenciamento de largura de banda e capacidade de links será plenamente atendido pela configuração administrativa e atribuição de perfis de vazão e prioridade aos links de conectividade, sendo aceita a solução que execute o balanceamento conforme esses parâmetros sem exigir recálculo autônomo e contínuo sem supervisão do administrador. **Está correto nosso entendimento?**

25. Protocolos de Sondagem de Qualidade de Links WAN (Subitem 5.1.11.6)

Entendemos que a verificação de integridade e qualidade dos enlaces de dados será considerada atendida quando a solução suportar sondagens de monitoramento ativas baseadas em protocolos padrão de mercado, contemplando obrigatoriamente ICMP (Ping) e TCP/DNS, ainda que não disponha da totalidade dos testes proprietários ou de nicho listados (como TWAMP ou MOS). **Está correto nosso entendimento?**

26. Critérios de Priorização de Roteamento SD-WAN (Subitem 5.1.11.8.2)

Entendemos que a seleção do melhor enlace para o tráfego crítico corporativo será considerada atendida quando baseada na mensuração contínua de latência, jitter e taxa de perda de pacotes (SLA de rede), sendo tais métricas tecnicamente suficientes para determinar a qualidade do link, ainda que o volume nominal de banda não seja critério automatizado direto de desvio. **Está correto nosso entendimento?**

27. Roteamento Baseado em Critério de Custo (Subitem 5.1.11.8.3)

Entendemos que a priorização por menor custo será atendida pela atribuição administrativa de pesos, prioridades e ordenação de preferência entre as interfaces e gateways no balanceamento SD-WAN, sendo dispensável a existência de uma variável numérica denominada textualmente "custo financeiro da interface". **Está correto nosso entendimento?**

28. Balanceamento em Túneis IPSec Agregados (Subitem 5.1.11.12)

Entendemos que a distribuição de tráfego corporativo entre múltiplos túneis VPN agregados será considerada satisfeita mediante o balanceamento por sessão e por fluxo de comunicação, mecanismo padrão da indústria que assegura integridade de entrega e previne problemas de entrega de pacotes fora de ordem inerentes ao balanceamento por pacote individual. **Está correto nosso entendimento?**

29. Topologia Dinâmica de Túneis VPN (Subitem 5.1.11.13)

Entendemos que a interconexão segura entre matriz e filiais será atendida mediante o estabelecimento de arquiteturas de VPN consolidadas e gerenciadas centralmente (como Hub-and-Spoke ou malha estruturada), sendo aceita a solução ainda que a negociação transitória de túneis sob demanda entre filiais dependa da infraestrutura configurada. **Está correto nosso entendimento?**

30. Mitigação de Perda de Pacotes e Continuidade de Links (Subitem 5.1.11.14)

Entendemos que a garantia de qualidade para aplicações sensíveis será atendida por políticas avançadas de QoS, priorização de filas e comutação rápida e automatizada (failover transparente) entre os links disponíveis com base nas métricas de SLA, sendo aceita a solução sem a exigência mandatória de duplicação simultânea de pacotes idênticos em múltiplos links. **Está correto nosso entendimento?**

31. Mecanismos de Correção de Erros de Enlace — FEC (Subitem 5.1.11.15)

Entendemos que a robustez e a resiliência na transmissão de dados em enlaces degradados serão atendidas pelos mecanismos de monitoramento contínuo de perda de pacotes com failover automático e técnicas de controle de congestionamento, sem que a tecnologia específica de Forward Error Correction (FEC) sobre o túnel VPN seja fator desclassificatório. **Está correto nosso entendimento?**

32. Persistência de Balanceamento de Links por IP (Subitens 5.1.11.20 e 5.1.11.21)

Entendemos que a distribuição balanceada de tráfego entre conexões WAN será atendida mediante persistência de sessão e amarração baseada em endereço IP de origem, IP de destino e portas de serviço, garantindo a estabilidade das aplicações que exigem afinidade de conexão, ainda que a documentação técnica não denomine essa função expressamente como "algoritmo de hash de IP". **Está correto nosso entendimento?**

33. Suporte a Conectividade Celular de Backup (Subitem 5.1.11.23)

Entendemos que a provisão de contingência de conectividade via rede móvel (3G/4G) poderá ser implementada por meio de roteadores/gateways celulares dedicados de padrão corporativo conectados a portas Ethernet padrão do firewall com políticas de failover automático, não sendo obrigatória a conexão física direta de modem em formato USB ao equipamento. **Está correto nosso entendimento?**

34. Extração de informações de desempenho das verificações de saúde via REST API (Subitem 5.1.11.24)

O subitem 5.1.11.24 exige que seja possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo a consolidação de tais informações em aplicação terceira.

Entendemos que a finalidade do requisito é assegurar a integração da solução com ferramentas de monitoramento e orquestração de terceiros, permitindo a coleta centralizada das informações de saúde e desempenho dos equipamentos e dos enlaces. Nesse sentido, entendemos que essa finalidade será considerada atendida quando a solução disponibilizar API documentada para consulta de status e configuração, complementada por mecanismos padrão de exportação de dados operacionais (SNMP, logs estruturados e integração com plataforma de gerenciamento central com APIs próprias), permitindo a consolidação das informações de desempenho e saúde em aplicação terceira, ainda que não exista endpoint REST dedicado e exclusivo para cada métrica individual das verificações de saúde. **Está correto nosso entendimento?**

35. Capacidade Simultânea de Túneis de Acesso Remoto VPN (Subitem 5.2.1.6)

O subitem 5.2.1.6 exige, para o Item 01, no mínimo 50.000 túneis de clientes VPN IPSec simultâneos. Esse valor, em conjunto com a exigência de 2.000 túneis Site-to-Site (subitem 5.2.1.5), reproduz exatamente a proporção e os números do datasheet do equipamento FortiGate 400G, da Fortinet, que especifica 2.000 túneis Gateway-to-Gateway e 50.000 túneis Client-to-Gateway IPsec — uma coincidência que, somada aos demais parâmetros já apontados na constatação preliminar, reforça o direcionamento do certame para aquele fabricante específico.

Ademais, a desproporção técnica entre os dois valores — 2.000 túneis site-to-site contra 50.000 túneis client-to-site, uma relação de 25 vezes — não encontra justificativa em necessidades típicas de dimensionamento de firewall corporativo, sendo característica de engenharia de hardware específica de um único fabricante, a **Fortinet**. Registra-se, ainda, que o padrão de mercado mais utilizado para acesso remoto de usuários (client-to-site) é a tecnologia VPN SSL, e não VPN IPSec, sendo que mesmo soluções consolidadas de mercado não comprovam 50.000 túneis IPSec client-to-site simultâneos em equipamentos de porte compatível com os demais parâmetros do Item 01.

Entendemos que a finalidade do requisito é assegurar capacidade suficiente de acesso remoto simultâneo para os usuários da CONTRATANTE, e que essa capacidade será avaliada com base no dimensionamento real e nas necessidades efetivas da Administração, sendo aceita a comprovação por capacidade equivalente de túneis VPN (IPsec ou SSL) compatível com o porte do equipamento ofertado, sendo em torno de 12.000 túneis VPN IPSEC e 18.000 túneis VPN SSL, sem exigência de patamar mínimo desproporcional e direcionado a fabricante específico. **Está correto nosso entendimento?**

36. Composição e Modularidade das Interfaces do Item 01 (Subitens 5.2.1.10, 5.2.1.12, 5.2.1.13 e 5.2.1.14)

O subitem 5.2.1.10 exige 4 interfaces SFP28 de 25 Gigabit Ethernet; o subitem 5.2.1.12 exige 16 interfaces SFP de 1 Gigabit Ethernet; o subitem 5.2.1.13 exige 8 interfaces de 5 Gigabit Ethernet com conector RJ45; e o subitem 5.2.1.14 exige 1 interface dedicada de 2,5 Gigabit Ethernet RJ45 exclusiva para alta disponibilidade e 1 interface Gigabit Ethernet RJ45 dedicada ao gerenciamento.

Considerando que o arranjo rígido e cumulativo de portas físicas de velocidades atípicas (5GbE e 2,5GbE combinadas com 25GbE) reflete a engenharia física exclusiva do modelo FortiGate 400G, da Fortinet, e que interfaces 2,5GbE e 5GbE RJ45 são tipicamente empregadas em switches de acesso

para recepção de access points e estações de trabalho — e não em firewalls corporativos de borda —, entendemos que, para assegurar a ampla competitividade do certame e a aderência aos padrões de mercado, será admitida composição diferente de interfaces, desde que assegurada a capacidade agregada de conectividade e o atendimento à vazão do ambiente, nos seguintes termos:

(i) 2 (duas) interfaces SFP28 de 25 Gigabit Ethernet, admitida a utilização de 2 interfaces QSFP28 de 40 Gigabit Ethernet nativas do equipamento com divisão (breakout) das portas em membros de 25 Gigabit Ethernet para o mesmo fim;

(i.A) Considerando que o Firewall será instalado no mesmo ambiente físico do parque de switches da CONTRATANTE, a uma distância inferior a 5 (cinco) metros, entendemos que as 2 (duas) interfaces SFP28 de 25 Gigabit Ethernet poderão ser entregues por meio de cabos DAC (Direct Attach Copper) com conector QSFP28 em uma extremidade (Firewall) e conector SFP28 na outra (switch da CONTRATANTE), dispensando a utilização de transceivers ópticos nessa interconexão, em conformidade com a lista oficial de compatibilidade de cabos DAC do fabricante do firewall;

(ii) 4 (quatro) interfaces SFP+ de 10 Gigabit Ethernet, conforme já consta no TR;

(iii) 8 (oito) interfaces SFP de 1 Gigabit Ethernet, admitida a utilização de interfaces SFP+ de 10 Gigabit Ethernet com transceivers SFP de 1 Gigabit Ethernet;

(iv) 8 (oito) interfaces Gigabit Ethernet RJ45, em substituição às interfaces de 2,5GbE e 5GbE RJ45;

(v) 1 (uma) interface Gigabit Ethernet RJ45 dedicada ao gerenciamento, conforme padrão de mercado;

(vi) Implementação de alta disponibilidade (HA) por qualquer interface de alta capacidade disponível no equipamento (10 Gigabit Ethernet ou Gigabit Ethernet), sem exigência de porta fisicamente dedicada e exclusiva para essa finalidade;

(vii) Quanto aos transceivers, solicitamos esclarecer se a CONTRATANTE já dispõe, em seu parque, dos transceivers SFP28 (25 Gigabit Ethernet), SFP+ (10 Gigabit Ethernet) e SFP (1 Gigabit Ethernet) necessários à interconexão com o equipamento ofertado, ou se tais transceivers deverão ser fornecidos pelo licitante como parte integrante da proposta, de modo a assegurar a correta e completa implantação da solução e a isonomia entre os licitantes na composição dos preços. **Está correto nosso entendimento?**

37. Fator de Forma e Ocupação de Rack para o Item 01 (Subitem 5.2.1.16)

O subitem 5.2.1.16 exige que o equipamento do Item 01 ocupe, no máximo, 1 (uma) unidade de rack (1U), em combinação cumulativa com os patamares de desempenho especificados nos demais subitens (145 Gbps de throughput de firewall, 55 Gbps de VPN IPSec, 25 Gbps de IPS e as interfaces e túneis acima indicados).

Nesse sentido, entendemos que a exigência cumulativa de fator de forma 1U com esse patamar de desempenho reflete a engenharia física exclusiva do modelo **FortiGate 400G, da Fortinet**, que combina essas características em chassis de 1U — reforçando os indícios de direcionamento já apontados na constatação preliminar, uma vez que a conjugação de tão alto desempenho com a ocupação de apenas 1U não é reproduzida por soluções equivalentes de outros fabricantes líderes de mercado, que oferecem essa faixa de desempenho em chassis de 2U.

Entendemos que a indicação do fator de forma de 1U consubstancia parâmetro de referência para planejamento de espaço físico, e não exigência técnica essencial, sendo plenamente aceita a oferta de equipamentos em chassi de 2U de padrão rack 19 polegadas, desde que o equipamento atenda ou supere todos os requisitos de processamento, vazão e segurança, dispondo a CONTRATANTE de espaço compatível em seus racks. **Está correto nosso entendimento?**

III. PARTE II — ITEM 03 (FERRAMENTA DE GESTÃO INTEGRADA, LOGS E RELATÓRIOS) — SUBITENS 5.3

38. Critério de Armazenamento para Solução de Gerenciamento em Nuvem (Subitens 5.3.3, 5.3.5.2 e 5.3.16)

O Termo de Referência autoriza expressamente, no subitem 5.3.5.2, o fornecimento da solução de gerenciamento e relatórios sob a modalidade em nuvem (SaaS), sem a necessidade de alocação de servidores ou appliances físicos no data center local. Diante disso, considerando que a solução sob plataforma de nuvem é contratada com capacidade de armazenamento de logs de 500 GB e garante a retenção de dados históricos e geração de relatórios consolidados por períodos de até 30 dias (1 mês), conforme o ciclo temporal exigido no subitem 5.3.16, entendemos que o requisito de armazenamento mínimo de 500 GB será avaliado pela capacidade de retenção de logs contratada e pelo período de retenção de 30 dias na nuvem do fabricante, não sendo exigida a apresentação de métrica de disco rígido físico local. **Está correto nosso entendimento?**

39. Personalização e Identidade Visual de Relatórios Administrativos (Subitem 5.3.14)

Entendemos que o requisito de customização e inserção de logotipo será considerado atendido quando a plataforma permitir a inclusão de dados institucionais e personalização de identidade visual nos relatórios gerados por meio de suas ferramentas e parametrizações nativas, ainda que o procedimento técnico de diagramação e inclusão de imagem difira de softwares instalados localmente. **Está correto nosso entendimento?**

IV. PARTE III — ITEM 04 (PROTEÇÃO DE SERVIDORES CONTRA EXPLORAÇÃO DE VULNERABILIDADES) — SUBITENS 5.4

40. Constatação Preliminar — Indícios de Direcionamento Técnico para a Plataforma Trend Micro

Da análise sistemática dos subitens 5.4.1 a 5.4.68 do Termo de Referência, constata-se a exigência cumulativa de funcionalidades e terminologias altamente peculiares — tais como inspeção de pacotes por frame type e flags TCP no host, módulo proprietário denominado "Log Inspection", controle de integridade de arquivos com modelos de hash específicos (MD5/SHA1/SHA256), regras de proteção contra vulnerabilidades com mecanismo de varredura atrelado a IDs de regras proprietárias, isolamento de interfaces com bypass de rastreamento e conectores legados voltados a VMware vCloud. Essa estrutura reflete, com extrema fidelidade conceitual e textual, a arquitetura fechada da linha de produtos **Deep Security / Trend Vision One, da fabricante Trend Micro**.

A imposição de requisitos aderentes a uma solução proprietária específica, em detrimento dos conceitos modernos de plataformas de Detecção e Resposta Estendidas (XDR) com recursos avançados de postura e mitigação de vulnerabilidades, configura evidente restrição ao caráter competitivo do certame, em manifesta contrariedade ao art. 9º, inciso III, e ao art. 25 da Lei Federal nº 14.133/2021, além de desrespeitar a excepcionalidade da padronização de marcas prevista no art. 41 do mesmo diploma. Solicita-se, assim, que a Administração confirme a ampla aceitação de soluções de mercado baseadas em plataformas XDR de última geração que entreguem a proteção e visibilidade requeridas, promovendo a isonomia do processo. **Está correto nosso entendimento?**

41. Arquitetura da Solução e Gerenciamento em Nuvem (Subitens 5.4.1, 5.4.4, 5.4.5, 5.4.8 e 5.4.18)

Entendemos que será aceita solução baseada em plataforma de XDR corporativa de última geração, provida em console de gerenciamento unificada em nuvem (SaaS) fornecida pelo próprio fabricante, operando por meio de agentes leves instalados nos sistemas operacionais dos servidores e entregando proteção multicamada, telemetria contínua e resposta a incidentes, ainda que determinados procedimentos técnicos internos difiram da arquitetura de softwares legados de proteção de servidores. **Está correto nosso entendimento?**

42. Matriz de Suporte a Sistemas Operacionais (Subitens 5.4.2, 5.4.66.1 e 5.4.67.1)

Considerando que o edital faz menção a sistemas operacionais Unix legados ou de baixíssima incidência no mercado público (como Solaris 11.4, CloudLinux, AIX e HP-UX), entendemos que o requisito destina-se a garantir a proteção do parque de servidores em produção da CONTRATANTE, sendo plenamente aceita a solução cuja matriz oficial de suporte contemple os sistemas operacionais corporativos modernos em uso (famílias Windows Server 2016, 2019 e 2022, e as principais distribuições Linux corporativas, tais como RHEL, CentOS, Oracle Linux, SUSE, Ubuntu e Debian). **Está correto nosso entendimento?**

43. Proteção de Ambientes Virtualizados e Nuvens Públicas (Subitens 5.4.3, 5.4.7 e 5.4.55)

Entendemos que a proteção de cargas de trabalho (workloads) em ambientes VMware e nuvens públicas (AWS, Azure e Google Cloud) será plenamente atendida pela instalação do agente de proteção diretamente no sistema operacional convidado (Guest OS) das máquinas virtuais e instâncias de nuvem, proporcionando monitoramento contínuo e resposta a ameaças sem a necessidade de appliances virtuais intermediários no hypervisor ou conectores de orquestração via VMware vCloud. **Está correto nosso entendimento?**

44. Métodos de Distribuição e Implantação de Agentes (Subitens 5.4.9, 5.4.27 e 5.4.28)

Entendemos que a implantação automatizada dos agentes será considerada plenamente atendida mediante o uso de ferramentas consolidadas de gerenciamento de infraestrutura (como Microsoft Endpoint Configuration Manager/SCCM, Group Policy Objects — GPO), pacotes de instalação padrão (MSI para Windows e RPM/DEB para Linux) e scripts de automação via PowerShell ou Shell Script, sendo prescindível o suporte nominal a ferramentas em desuso como Novell ZenWorks ou Puppet. **Está correto nosso entendimento?**

45. Mecanismos de Autenticação Administrativa (Subitens 5.4.6 e 5.4.19)

Entendemos que a segurança no acesso administrativo à console será assegurada por mecanismos de autenticação forte com Múltiplo Fator de Autenticação (MFA), integração e federação de identidade via provedores padrão (IdP / SAML / Azure AD), controle de acesso baseado em funções (RBAC) e tráfego integralmente criptografado via HTTPS/TLS, não sendo obrigatória a exigência de certificado digital de cliente instalado no navegador. **Está correto nosso entendimento?**

46. Geração e Formatos de Exportação de Relatórios (Subitens 5.4.15, 5.4.16, 5.4.17 e 5.4.43)

Entendemos que a entrega de relatórios e dados para auditoria será considerada atendida mediante a disponibilização das informações em painéis interativos (dashboards), consultas sob demanda e exportação nos formatos padrão de mercado (PDF e formatos estruturados como CSV/JSON), com proteção e controle de acesso nativos da plataforma, sendo dispensável o fornecimento concomitante nos formatos RTF e XLS ou proteção por senha individualizada por arquivo. **Está correto nosso entendimento?**

47. Atualização Centralizada de Motores e Assinaturas (Subitens 5.4.13, 5.4.26 e 5.4.44 a 5.4.47)

Entendemos que a manutenção e atualização contínua da inteligência de segurança dos agentes será realizada de forma automatizada, silenciosa e segura diretamente a partir da nuvem do fabricante, sem a necessidade mandatória de implantação de servidores intermediários locais (relays/distribuidores), repositórios manuais de assinaturas ou procedimentos manuais de rollback. **Está correto nosso entendimento?**

48. Granularidade de Permissões Administrativas (Subitens 5.4.21, 5.4.22 e 5.4.50)

Entendemos que a segregação de privilégios será plenamente atendida pela criação de perfis administrativos personalizados na console em nuvem, permitindo definir papéis com privilégios de leitura, escrita, resposta a incidentes e gerenciamento de políticas segmentados por grupos de servidores ou unidades operacionais, ainda que a plataforma não adote a estrutura de delegação restrita a um único computador individual. **Está correto nosso entendimento?**

49. Integração e Exportação de Eventos para SIEM/SOAR (Subitens 5.4.41 e 5.4.42)

Entendemos que a capacidade de integração da plataforma com ecossistemas externos de segurança (como Splunk, IBM QRadar, Microsoft Sentinel, HP ArcSight, servidores Syslog e serviços de mensageria em nuvem) será atendida por meio da disponibilização de APIs RESTful documentadas e conectores universais de extração e encaminhamento contínuo de logs e telemetria de segurança. **Está correto nosso entendimento?**

50. Visibilidade e Monitoramento de Ambientes de Containers (Subitem 5.4.20)

Entendemos que a segurança em servidores que executam contêineres será considerada atendida quando o agente do host monitorar continuamente processos anômalos, chamadas de sistema, tráfego e desvios de comportamento nos nós computacionais, consolidando a telemetria na console de XDR, ainda que a solução não possua um módulo isolado denominado "proteção contra ataques entre containers". **Está correto nosso entendimento?**

51. Controle e Isolamento Lógico de Comunicações do Servidor (Subitens 5.4.38, 5.4.39 e 5.4.40)

Entendemos que o requisito voltado à contenção e resposta a incidentes será atendido pela capacidade da solução de isolar o servidor da rede corporativa mantendo apenas o canal de gerência seguro para mitigação, bem como pela aplicação centralizada de políticas de controle de tráfego e exclusões de inspeção no agente, sendo desnecessária a desativação de placas físicas de rede ou a adoção do termo "bypass completo de rastreamento". **Está correto nosso entendimento?**

52. Gerenciamento e Controle de Firewall de Host (Subitem 5.4.64)

Entendemos que o controle do fluxo de rede nos servidores será plenamente atendido pela aplicação centralizada de políticas de controle de portas, serviços, endereços IP e governança do mecanismo de firewall nativo do sistema operacional pelo agente de segurança e exclusivamente para SOs Windows, sendo prescindível a implementação de filtros de camada de enlace (frame type), inspeção de flags TCP de baixo nível ou bloqueio específico de tipos de varredura com nomenclaturas idênticas às descritas no edital, de forma a afastar o direcionamento técnico para a solução da TrendMicro, aumentando a competitividade do certame. **Está correto nosso entendimento?**

53. Proteção contra Exploração de Aplicações em Nível de Host (Subitens 5.4.65.9 a 5.4.65.14)

Entendemos que a segurança de servidores contra invasões e exploração de código malicioso será assegurada por mecanismos de prevenção de exploits (Anti-Exploit), proteção de memória, bloqueio de técnicas de evasão e inspeção comportamental executados pelo agente de segurança do servidor, sendo tecnicamente compreendido que a inspeção aprofundada de requisições web em camada 7 com funções de WAF é atribuição do módulo correspondente da infraestrutura de borda (Item 05). **Está correto nosso entendimento?**

54. Análise, Postura e Mitigação de Vulnerabilidades no Servidor (Subitens 5.4.34, 5.4.35, 5.4.36, 5.4.37 e 5.4.65)

Considerando que as plataformas XDR modernas dispõem de capacidade nativa de avaliação contínua de vulnerabilidades, inventário de softwares e telemetria de exposição, identificando com precisão pacotes desatualizados, lacunas de correção (patching) e configurações de risco diretamente pela telemetria do agente e permitindo consultas detalhadas e ações de mitigação, entendemos que essa capacidade atende integralmente à finalidade do TR de identificação e proteção de vulnerabilidades, sem que haja a exigência mandatória de um módulo independente de varredura ativa de rede com atribuição automática de regras proprietárias de IDS/IPS baseadas em catálogo fechado, de forma a afastar o direcionamento técnico para a solução da TrendMicro, aumentando a competitividade do certame. **Está correto nosso entendimento?**

55. Mecanismos de Coleta e Registro de Evidências Forenses (Subitens 5.4.65.6 e 5.4.65.19)

Entendemos que o requisito voltado à investigação e análise forense será atendido pela capacidade da plataforma XDR de registrar, correlacionar e disponibilizar detalhadamente a cadeia de ataque, comandos executados, processos envolvidos, conexões de rede e artefatos do incidente na console centralizada, sendo dispensável a captura bruta e contínua de tráfego de rede em formato PCAP para os eventos detectados. **Está correto nosso entendimento?**

56. Criação de Regras e Consultas de Detecção Customizadas (Subitens 5.4.65.7, 5.4.65.16, 5.4.65.17, 5.4.65.22, 5.4.57 e 5.4.58)

Entendemos que a capacidade de personalização de defesas será plenamente atendida pela criação de regras de detecção personalizadas, consultas avançadas de telemetria na base de dados de XDR e bloqueio customizado de indicadores de comprometimento (IoCs), sendo dispensável o suporte à edição de assinaturas em formato XML proprietário ou a disponibilização de manuais estruturados denominados "cookbooks", sendo a severidade classificada segundo os motores de inteligência da plataforma. **Está correto nosso entendimento?**

57. Monitoramento de Integridade e Análise de Eventos do Sistema (Subitens 5.4.66 e 5.4.67)

Entendemos que a governança de integridade será plenamente atendida pelo monitoramento contínuo de alterações críticas no registro, arquivos de sistema e diretórios sensíveis nos servidores Windows e Linux suportados, conjugado à coleta e análise contínua dos logs de segurança dos sistemas operacionais pela console de XDR, sendo dispensável a existência de um módulo isolado nomeado "Log Inspection" para análise de aplicações legadas de terceiros ou suporte a sistemas Unix descontinuados (AIX, Solaris e HP-UX), de forma a afastar o direcionamento técnico para a solução da TrendMicro, aumentando a competitividade do certame. **Está correto nosso entendimento?**

58. Controle de Aplicações e Proteção Antimalware com Inteligência Artificial (Subitens 5.4.62 e 5.4.68)

Entendemos que a proteção do ambiente será considerada plenamente atendida pela combinação de motores antimalware de alta precisão com aprendizado de máquina (Machine Learning), inteligência de ameaças em tempo real, proteção contra ransomware com reversão automática de arquivos comprometidos e controle de execução de aplicativos por categorias e políticas corporativas, sendo dispensável a exigência de bloqueio exclusivo por hashes estáticos (MD5/SHA1/SHA256) ou a comprovação de métricas fixas de camadas de descompressão de arquivos compactados. **Está correto nosso entendimento?**

V. PARTE IV — ITEM 05 (WAF — FIREWALL DE APLICAÇÃO WEB) — SUBITENS 5.5

59. Constatação Preliminar — Indícios de Direcionamento Técnico para a Linha FortiWeb

A leitura exaustiva do Item 5.5 do Termo de Referência (subitens 5.5.1 a 5.5.65) revela a transposição literal de funcionalidades, nomenclaturas e rotinas operacionais presentes de forma exclusiva e característica na documentação técnica do appliance de WAF FortiWeb, de fabricação da Fortinet. Destacam-se as exigências de "modelo positivo de segurança" atrelado a perfis automatizados de autoaprendizado (Application Learning), mitigação comportamental de DDoS em camada 7 com terminologias proprietárias, assinatura digital de cookies com criptografia customizada, edição de URLs no corpo da resposta e detecção de ataques de força bruta baseada em uma matriz cumulativa de múltiplos indicadores (tempo de resposta, taxa de transações por segundo — TPS por IP e expressões regulares em páginas de erro customizadas).

A imposição de uma arquitetura proprietária tão estrita para a proteção de aplicações web, além de injustificada sob o ponto de vista da entrega de segurança efetiva (já que o objetivo é proteger as aplicações contra os riscos mapeados, mormente o OWASP Top 10), fere frontalmente o art. 9º, inciso III, o art. 25 e o art. 41 da Lei Federal nº 14.133/2021. Deste modo, requer-se que a Administração esclareça se serão admitidas propostas baseadas em soluções consolidadas de WAF corporativo que executem a proteção profunda e completa das aplicações publicadas por meio de mecanismos robustos e modernos de proxy reverso e regras avançadas de proteção, preservando a competitividade do certame. **Está correto nosso entendimento?**

60. Modalidade e Integração da Solução de Proteção WAF (Subitens 5.5.1 e 5.5.6)

Considerando que a expressão "appliance dedicado" constante do subitem 5.5.1 qualifica a função de segurança de proteção a aplicações web e não a obrigatoriedade de hardware exclusivo e isolado, entendemos que será plenamente aceita a oferta de solução de WAF que opere como proxy reverso integrado à plataforma de firewall corporativo (atendendo ao Item 5.5 como módulo de proteção de servidores web para proteção por firewall de aplicações web), entregando funcionalidades de segurança, inspeção e mitigação. **Está correto nosso entendimento?**

61. Mitigação de Ataques de Camada 7, Bots e Automação (Subitens 5.5.9, 5.5.17 e 5.5.45.17)

Entendemos que a proteção contra negação de serviço em nível de aplicação (DDoS L7), Web Scraping, crawlers maliciosos e automações não autorizadas será considerada atendida quando a solução disponibilizar mecanismos nativos de limitação de taxa de requisições (rate limiting), controle de clientes automatizados e filtragem de requisições anômalas, ainda que a documentação técnica do fabricante não empregue especificamente as expressões "análise comportamental" ou "machine learning". **Está correto nosso entendimento?**

62. Registro e Análise de Requisições HTTP em Incidentes (Subitem 5.5.10)

Entendemos que a finalidade de viabilizar a auditoria técnica e o troubleshooting de requisições será plenamente satisfeita pelo registro estruturado em logs das requisições HTTP/HTTPS bloqueadas contendo cabeçalhos, payloads, métodos e parâmetros disparadores da violação, sendo prescindível a geração e armazenamento automático de um arquivo de captura bruta denominado "TCP Dump" para cada evento detectado. **Está correto nosso entendimento?**

63. Suporte a Protocolos de Navegação Web (Subitem 5.5.11)

O subitem 5.5.11 exige análise dos protocolos HTTP/0.9, HTTP/1.0, HTTP/1.1 e HTTP/2. Considerando a evolução dos protocolos HTTP e a necessidade de compatibilidade com as aplicações web efetivamente utilizadas pela CONTRATANTE, entendemos que a finalidade do requisito é assegurar a capacidade de inspecionar e proteger as aplicações web publicadas, sendo considerada atendida a exigência mediante o suporte comprovado aos protocolos HTTP/1.0 e HTTP/1.1, padrões amplamente consolidados e suficientes para as aplicações corporativas atuais. Entendemos, ainda, que não se mostra necessária a manutenção de compatibilidade com o protocolo obsoleto e inseguro HTTP/0.9, nem a exigência de suporte ao protocolo HTTP/2, cuja adoção depende da aplicação

publicada e não constitui requisito de segurança da solução de proteção de aplicações web. **Está correto nosso entendimento?**

64. Implementação de Mecanismos de Proteção e Políticas por Aplicação (Subitens 5.5.14, 5.5.20, 5.5.26 e 5.5.46)

Entendemos que o objetivo de garantir a integridade dos dados e impedir a adulteração de parâmetros será plenamente atendido por políticas de segurança aplicadas por aplicação web/URL publicada, incluindo controle rígido de métodos HTTP permitidos, proteção de campos de formulários, verificação de conformidade de protocolos e bloqueio de caracteres ilegais, ainda que o fabricante não utilize a denominação formal de "modelo positivo de segurança" ou "perfil de utilização aprendido". **Está correto nosso entendimento?**

65. Mecanismos de Ajuste e Aprendizado de Tráfego de Aplicações (Subitens 5.5.34 a 5.5.36, 5.5.42, 5.5.48, 5.5.54 e 5.5.57)

Entendemos que a customização e ajuste fino das regras de proteção das aplicações corporativas serão assegurados pela capacidade da solução de operar em modo de monitoramento/aprendizado durante o tráfego de homologação ou produção, permitindo ao administrador identificar falsos positivos e refinar as regras e exceções de segurança, ainda que a dinâmica de criação de regras difira das rotinas automatizadas do módulo "Application Learning" proprietário do **FortiWeb da Fortinet**, de forma a afastar o direcionamento técnico para a solução da Fortinet, aumentando a competitividade do certame. **Está correto nosso entendimento?**

66. Modalidades de Bloqueio, Resposta e Mitigação de Ameaças (Subitens 5.5.21 a 5.5.25)

Entendemos que a exigência de interrupção tempestiva de ataques será atendida pelo bloqueio imediato das conexões ilegítimas em nível de proxy reverso, com o envio de páginas de resposta ou códigos de status HTTP apropriados ao cliente e o bloqueio automático temporário de endereços IP de origem maliciosos por meio de políticas de contenção, ainda que tais rotinas não utilizem o rótulo formal de "bloqueio com intermediação e interrupção". **Está correto nosso entendimento?**

67. Registro Detalhado de Ataques e Rastreabilidade de Sessão (Subitens 5.5.27 e 5.5.28)

Entendemos que a rastreabilidade dos eventos de segurança será plenamente atendida pelo armazenamento detalhado em logs contendo a regra violada, o campo atacado, a data e hora do evento, o IP de origem e os dados de contexto da requisição, sendo essas informações consultáveis e exportáveis por meio das ferramentas de auditoria e relatórios da plataforma. **Está correto nosso entendimento?**

68. Proteção de Cabeçalhos, Cookies e Dados de Aplicação (Subitens 5.5.29, 5.5.30 e 5.5.31)

Entendemos que: (i) o tráfego compactado (gzip/deflate) será tratado de forma nativa e transparente pelo mecanismo de proxy reverso; (ii) a proteção de cookies de sessão será atendida pela aplicação de atributos de segurança (como HttpOnly, Secure e escopo de domínio/caminho) nas políticas de publicação web; (iii) o direcionamento de URLs será realizado pelo mecanismo de publicação e mapeamento de caminhos do proxy reverso; e (iv) a proteção de banco de dados refere-se à blindagem das aplicações contra injeção de comandos SQL (SQL Injection), não implicando na exigência de monitoramento de atividade interna de banco de dados (DAM) no SGBD. **Está correto nosso entendimento?**

69. Detecção e Bloqueio de Ataques de Força Bruta (Subitens 5.5.39, 5.5.40 e 5.5.41)

Entendemos que a mitigação de ataques de força bruta, tentativas massivas de autenticação e preenchimento de credenciais será considerada plenamente atendida por mecanismos de limitação de taxa de requisições por IP, controle de concorrência de sessões e regras de inspeção em URLs de autenticação, sendo desnecessária a obrigatoriedade do atendimento cumulativo e estrito a todos os parâmetros nominais descritos (como cálculo de tempo de resposta em milissegundos ou casamento de expressão regular em páginas de erro). **Está correto nosso entendimento?**

70. Cobertura Abrangente contra Ameaças Web e OWASP Top 10 (Subitens 5.5.43, 5.5.45, 5.5.50, 5.5.51, 5.5.53, 5.5.59 e 5.5.60)

Entendemos que a exigência de segurança contra vulnerabilidades web será integralmente satisfeita pela proteção ativa contra a totalidade dos riscos críticos listados no OWASP Top 10 (incluindo SQL Injection, Cross-Site Scripting — XSS, Cross-Site Request Forgery — CSRF, injeção de comandos, adulteração de parâmetros e XML/SOAP malformado) por meio de motores consolidados de inspeção e regras gerenciadas continuamente atualizadas pelo fabricante, com total flexibilidade para a criação de regras e exceções personalizadas pelo administrador. **Está correto nosso entendimento?**

71. Retenção de Dados Históricos, Exportação e Relatórios de WAF (Subitens 5.5.55, 5.5.56, 5.5.63, 5.5.64 e 5.5.65)

Entendemos que a governança, auditoria e geração de relatórios de segurança da solução de WAF serão atendidas pela visualização centralizada de estatísticas de conexões, geolocalização de origens e eventos de ameaças por meio de painéis dinâmicos e emissão de relatórios com retenção mínima de 30 dias contratada e capacidade de exportação em PDF ou CSV, ainda que a diagramação visual difira de gráficos proprietários do fabricante Fortinet, de forma a afastar o direcionamento técnico para a solução da Fortinet, aumentando a competitividade do certame. **Está correto nosso entendimento?**

VI. REQUERIMENTO FINAL

Ante todo o exposto, pugna-se pelo conhecimento e integral acolhimento do presente Pedido de Esclarecimento, requerendo-se que as respostas e os posicionamentos técnicos da Administração Pública sejam formalizados de maneira clara e transparente e devidamente publicados nos autos do certame licitatório e nos sistemas oficiais, no prazo e na forma estipulados pelo **art. 164, parágrafo único, da Lei Federal nº 14.133/2021**, garantindo-se a indispensável segurança jurídica aos licitantes.

Reitera-se o firme compromisso da requerente em contribuir com a Administração Pública Municipal na obtenção de uma contratação pautada na excelência técnica, na economicidade, na estrita legalidade e na mais ampla competitividade, assegurando a melhor relação custo-benefício para COMPANHIA DE DESENVOLVIMENTO DE INFORMÁTICA DE UBERABA — CODIUB.

Termos em que pede e espera deferimento.

Atenciosamente,

Security Data
Tecnologia da Informação.
www.securitydata.tec.br

Comercial
(61) 99445-6263 | 3550-6869
comercial@securitydata.tec.br