



GOVERNO DO ESTADO DE RONDÔNIA

Secretaria de Estado da Educação - SEDUC

Coordenadoria de Tecnologia da Informação e Comunicação - SEDUC-COTIC

Parecer nº 63/2026/SEDUC-COTIC

Processo Administrativo nº: 0029.003939/2025-74

Pregão Eletrônico nº: 212/2026/SUPEL/RO

Interessado: Secretaria de Estado da Educação – SEDUC/RO

Assunto: Análise Técnica de Proposta e Diligência – 2º Colocado (THS Tecnologia, Informação e Comunicação LTDA.)

PARECER TÉCNICO

À: Gerência de Contratações de Serviços - SEDUC-GCS

ASSUNTO: Análise de atendimento aos requisitos técnicos do Termo de Referência (SEI nº 74267331) referentes à Proposta THS.

1. DO NÃO ATENDIMENTO AOS REQUISITOS DE VPN SSL – ITEM 7.2.2 DO TERMO DE REFERÊNCIA

ITENS NÃO ATENDIDOS:

- **Item 7.2.2-1:** "Deverá implementar as funcionalidades de Single Sign-on e VPN-SSL, com no mínimo os seguintes recursos:"
- **Item 7.2.2-2:** "Deve possuir o modo "Portal" onde a solução se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;"
- **Item 7.2.2-3:** "Deve possuir o modo "Network", onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna."
- **Item 7.2.2-4:** "Deverá possuir ativo o controle de, no mínimo, 500 usuários concorrentes, e deverá vir com todo o licenciamento necessário para ativação desses 500 usuários;"
- **Item 7.2.2-5:** "Deverá possuir cliente VPN SSL para pelo menos os sistemas operacionais Windows, Linux e MacOS;"
- **Item 7.2.2-6:** "Deverá possuir validação da estação de trabalho do usuário, para pelo menos: Sistema Operacional, Antivírus e Firewall."
- **Item 7.2.2-19:** "Deve possuir capacidade para definir lease pool que contenha endereços IP a serem designados aos usuários com acesso a rede;"

DOCUMENTO(S) ANALISADO(S):

18 e 19 A10 Networks – Thunder ADC Data Sheet (A10-DS-15100-EN-63, julho/2026), páginas 6,

<https://www.a10networks.com/wp-content/uploads/A10-DS-Thunder-ADC.pdf>

A10 Networks – Solution Brief: Load Balancing Pulse Secure SSL VPN Deployments (A10-SB-19127-EN)

<https://www.a10networks.com/wp-content/uploads/A10-SB-19127-EN.pdf>

ANÁLISE TÉCNICA:

A exigência do item 7.2.2-1 é expressa e cumulativa: Single Sign-on e VPN-SSL. O atendimento apenas da parte de Single Sign-On não supre o requisito.

O equipamento ofertado, Thunder 7460S, integra a linha Thunder ADC. O datasheet oficial mais recente dessa linha, no qual constam as especificações do próprio 7460S, descreve na página 6, seção "SSO and Application Authentication", o único módulo de controle de acesso da linha: o Application Access Management (AAM).

O módulo é apresentado como responsável por aplicar autenticação e autorização às aplicações, com métodos como LDAP, RADIUS, RSA SecurID, TDS SQL, SAML e Kerberos. Não há qualquer menção a VPN, túnel SSL, cliente VPN, modo Portal ou modo Network.



SSO

and Application Authentication

The integrated application access management (AAM) module optimizes and enforces authentication and authorization to applications.

The module integrates with authentication servers, identity data stores, identity providers (IdPs) and applications to authenticate users and enforce access privileges. Common AAA and single sign-on (SSO) methods include LDAP, RADIUS, RSA SecurID, TDS SQL, SAML and Kerberos.

AAM interfaces to OCSP responders to validate client certificate status, as well as to Microsoft Active Directory for SharePoint and Outlook Web Access users.

Referência: documento 1, página 6.

Nas páginas 18 e 19, seção "Detailed Feature List", o fabricante relaciona todas as funcionalidades da linha. Na categoria "Application Security", os itens relativos a acesso são exclusivamente: AAM (SAML, WIA, Kerberos, NTLM, TDS SQL Logon, LDAP, RADIUS, Basic, OCSP stapling, HTML Form-based), suporte a auditoria via RADIUS, relay de autenticação SSO e autenticação para Microsoft SharePoint, Outlook Web Access e outras aplicações.

Application Security

- Next-Generation Web Application Firewall (Next-Gen WAF)
 - DNS application firewall (DAF)
 - Integrated DDoS protection for application services
 - Hardware-based DDoS protection
 - Application Access Management (AAM) – SAML, WIA, Kerberos, NTLM, TDS SQL Logon, LDAP, RADIUS, Basic, OCSP stapling, HTML Form-based
 - AAM RADIUS-based audit support
 - Single sign-on (SSO) authentication relay
 - Authentication for Microsoft SharePoint, Outlook Web Access, and other packaged and custom applications
 - Comprehensive SSL/TLS support
 - TLS 1.2 and TLS 1.3
 - Perfect Forward Secrecy (PFS) with Elliptic Curve Diffie-Hellman Exchange (ECDHE) and other Elliptic Curve Cryptography (ECC) ciphers
 - AES-NI and GCM ciphers
 - Post-Quantum Cryptographic (PQC) - Hybrid-KEM
 - IP anomaly detection
-
- DDoS attack detection and prevention using zero-day source behavior attack detection and recognition (ZBAR)
 - Defend against HTTP request smuggling
 - Connection rate limiting/connection limiting
 - Bandwidth rate limiting per source IP
 - Dynamically add IPs to black-white lists
 - Support for Simple Certificate Enrollment Protocol (SCEP)
 - ACME client support for automatic certificate renewal

Referência: documento 1, páginas 18 e 19.

A lista completa de funcionalidades não contém nenhuma referência a:

- VPN SSL ou VPN de acesso remoto;
- Cliente VPN para qualquer sistema operacional;
- Modo Portal ou modo Network, nem equivalentes como "web portal", "network access" ou "full tunnel";
- Validação de postura da estação (endpoint check / host checking);
- Lease pool ou atribuição de endereço IP a usuários remotos;
- Licenciamento por usuários concorrentes de VPN.

Ou seja, o documento em que o fabricante descreve exhaustivamente as capacidades do produto ofertado não relaciona a funcionalidade exigida.

O Solution Brief A10-SB-19127-EN confirma essa conclusão. Nele, o próprio fabricante posiciona o Thunder ADC como balanceador de carga de gateways de VPN SSL de outro fabricante (Pulse Secure / Ivanti Connect Secure). A arquitetura descrita usa Thunder ADCs com Global Server Load Balancing (GSLB) para distribuir os usuários entre os nós Pulse Connect Secure, sob uma URL virtual única.

LOAD BALANCING PULSE SECURE SSL VPN DEPLOYMENTS

Provide Scalable, Reliable and Secure Remote Access

Challenge:
Remote users require secure and uninterrupted access to corporate resources.

Solution:
A10 Thunder ADC load balances Pulse Connect Secure deployments for High Availability and to increase overall SSL VPN capacity.

Benefits:

- Maximize uptime and scale with best-in-class load balancing and clustering
- Detect network or service failures with advanced health monitoring
- Extend secure remote access to a wide array of PC and smart device OS platforms
- Lower total cost of ownership (TCO) by using a single SSL VPN client across various desktops and mobile devices

Mobile Users Require Secure Always-On Network Access

SSL VPN technology has become the de facto standard for remote access to enterprise network resources. SSL VPN solutions have attained widespread adoption as a low-cost, more easily configured and managed alternative to cumbersome, cost inefficient IPsec solutions.

With SSL VPN deployments, employees, partners and vendors can easily and securely access the enterprise network from remote locations without the need to install or maintain special software. Evolution of the technology over the last several years has yielded mature, highly configurable solutions such as Pulse Connect Secure (formerly Juniper Networks Secure Access).

Success Brings New Challenges

The success of SSL VPN has created its own challenges. As organizations continue to deploy the technology, the user base continues to grow accordingly. Organizations are faced with the need to scale SSL VPN deployments to meet ever increasing demand, while at the same time maintaining the availability, robustness and ease of use of the solution. Similar scalability and reliability challenges confront organizations wishing to deploy new SSL VPN solutions. To address the challenges facing legacy and greenfield global SSL VPN deployments, robust, reliable, high-performance load balancing is required.

Pulse Connect Secure SSL VPN and A10 Thunder Series Provide a Robust, Scalable Solution

A combined solution using Pulse Connect Secure and A10 Networks® Thunder™ ADC line of high-performance, next-generation application delivery controllers provides optimal SSL VPN service. The access and security features of Pulse Connect Secure are easily extended to a

Pulse Secure

Pulse Secure is a "new" company born from the sale of Juniper Networks Junos Pulse product line to Siris Capital, a leading private equity firm. Pulse Secure is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual

Referência: documento 2, páginas 1 e 3.

Se o equipamento tivesse VPN SSL nativa, não haveria razão para o fabricante publicar uma arquitetura de referência em que a VPN SSL é fornecida por produto de terceiros e o Thunder atua apenas no balanceamento. Nessa arquitetura, a função de VPN SSL é externa ao equipamento A10.

Também não é possível suprir essa ausência com produto de outro fabricante não ofertado na proposta, pois isso configuraria alteração da composição da solução após a abertura das propostas, o que é vedado.

CONCLUSÃO:

Ficou demonstrado, com base na documentação oficial do fabricante, que o Thunder ADC oferece apenas autenticação e SSO para aplicações web, que a lista completa de funcionalidades do produto não inclui VPN SSL e que o próprio fabricante trata a VPN SSL como função de produto de terceiros. A solução ofertada **não atende aos itens 7.2.2-1, 7.2.2-2, 7.2.2-3, 7.2.2-4, 7.2.2-5, 7.2.2-6 e 7.2.2-19.**

2. DO NÃO ATENDIMENTO AOS REQUISITOS DE TELEMETRIA – ITENS 7.1.2-33, 7.1.2-36 E 7.1.2-42 A 7.1.2-48

ITENS NÃO ATENDIDOS:

- **Item 7.1.2-33:** "Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:"
- **Item 7.1.2-36:** "Exportação de métricas de desempenho compatíveis com, pelo menos, os

sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, ElasticSearch, Fluentd, GCP Cloud Monitoring e Logging, Graphite, Kafka, Splunk e StatsD;"

- **Item 7.1.2-42:** "Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;"

- **Item 7.1.2-43:** "Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;"

- **Item 7.1.2-45:** "Deve incluir métricas de desempenho dos scripts de manipulação de tráfego, incluindo total de execuções, média de ciclos, máximo e mínimo de ciclos e falhas;"

- **Item 7.1.2-46:** "Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);"

- **Item 7.1.2-47:** "Deve incluir métricas do cluster, incluindo data de sincronização;"

- **Item 7.1.2-48:** "Deve incluir informações de data da última configuração aplicada;"

DOCUMENTO ANALISADO:

3. A10 Networks – Thunder Observability Agent (TOA) v3.0.0 – documentação oficial.

<https://github.com/a10networks/thunder-observability-agent>

ANÁLISE TÉCNICA:

O agente de telemetria da A10 é o Thunder Observability Agent (TOA). Segundo a documentação oficial do fabricante, ele não é integrado ao equipamento: trata-se de mecanismo autônomo, instalado externamente em servidores Linux, CentOS ou Ubuntu, como pacote Python ou contêiner Docker. Isso não atende ao item 7.1.2-33, que exige agente integrado.

A10's Thunder Observability Agent (TOA) - v3.0.0

The TOA is a lightweight autonomous data processing engine that can be externally installed and config TOA offers the following capabilities on Application Delivery Controller (ADC):

- Collects, processes, and publishes 14 Thunder metrics.
The default data collection frequency is 1 minute. Thunder metrics can be sent to the platform where
- Collects, processes, and publishes Thunder Syslogs.
The default data collection frequency is 1 minute. The logs can be published on various platforms li
Logs can be sent to any one platform at a time. For more information on Thunder logs, see Supported

Referência: documento 3.

A mesma documentação limita o agente a 14 métricas, enviadas a apenas uma plataforma por vez: uso de CPU, memória e disco, taxa de throughput, contagem de interfaces down, novas conexões, taxa de transações, contagem e percentual de servidores down, erros SSL, erros de servidor, total de sessões, taxa de pacotes e taxa de descarte de pacotes.

Documentation

[A10 TOA Documentation Site.](#)

Supported Thunder vADC Performance Metrics

1. CPU Usage Percentage (Data).
2. Memory Usage Percentage.
3. Disk Usage Percentage.
4. Throughput Rate (Global/BPS)
5. Interface Down Count (Data)
6. Total New Connection (Sec)
7. Transactions Rate (Sec)
8. Server Down Count
9. Server Down Percentage
10. SSL Errors Count
11. Server Errors Count
12. Total Session Count
13. Packet Rate (Sec) [Since ACOS 5.2.1-P7+]
14. Packet Drop Rate (Sec) [Since ACOS 5.2.1-P7+]

Referência: documento 3, seção de métricas suportadas.

Essa lista não contempla as métricas de criptografia (7.1.2-42), de certificados digitais (7.1.2-43), de desempenho dos scripts de manipulação de tráfego (7.1.2-45), as informações de inventário (7.1.2-46), as métricas de cluster com data de sincronização (7.1.2-47) nem a data da última configuração aplicada (7.1.2-48).

Quanto aos destinos de exportação, a documentação oficial relaciona como plataformas suportadas AWS, Azure, VMware, Splunk, ElasticSearch-Kibana, Prometheus-Grafana (PushGateway), Google Cloud Platform e Oracle Cloud Infrastructure. Não constam Amazon S3, Graphite, Kafka nem StatsD, todos exigidos nominalmente no item 7.1.2-36.

Supported Monitoring Platforms

1. AWS.
2. Azure.
3. VMware.
4. Splunk
5. ElasticSearch-Kibana
6. Prometheus-Grafana [PushGateway]
7. Google Cloud Platform (GCP)
8. Oracle Cloud Infrastructure (OCI)

Referência: documento [3](#), seção de plataformas suportadas.

CONCLUSÃO:

Ficou demonstrado que a solução ofertada **não atende aos itens 7.1.2-33, 7.1.2-36, 7.1.2-42, 7.1.2-43, 7.1.2-45, 7.1.2-46, 7.1.2-47 e 7.1.2-48.**

3. DO NÃO ATENDIMENTO AOS REQUISITOS DE ORQUESTRAÇÃO DE CONTÊINERES – ITENS 7.1.3-25 E 7.1.3-28

ITENS NÃO ATENDIDOS:

- **Item 7.1.3-25:** "Suportar, pelo menos, as plataformas Kubernetes "Vanilla", Red Hat OpenShift e VMware Tanzu;"
- **Item 7.1.3-28:** "Permitir a configuração através de objetos de serviço (Service) do tipo LoadBalancer na plataforma;"

DOCUMENTO ANALISADO:

4. A10 Networks – Thunder Kubernetes Connector (TKC) Documentation – repositório oficial

<https://github.com/a10networks/tkc-doc>

ANÁLISE TÉCNICA:

A integração da A10 com Kubernetes é feita pelo Thunder Kubernetes Connector (TKC). A documentação oficial do conector informa suporte a Kubernetes on-prem ou em nuvem (Azure AKS, AWS EKS e Oracle CE) e a OpenShift on-prem. O VMware Tanzu não consta entre as plataformas suportadas, o que caracteriza o não atendimento ao item 7.1.3-25.

Supportability for Kubernetes and OpenShift clusters

TKC with Thunder ADC is supported for Kubernetes on-prem or Kubernetes on Cloud for Azure AKS, AWS EKS and Oracle CE. TKC with Thunder ADC is also supported for OpenShift on-prem with advanced routing capabilities.

Referência: documento 4, seção "Supportability for Kubernetes and OpenShift clusters".

Quanto ao Service do tipo LoadBalancer, a documentação oficial trata a funcionalidade na seção intitulada "Service of type LoadBalancer with IPAM for on-prem Kubernetes Cluster (Future versions of TKC)". Ou seja, o próprio fabricante a apresenta como recurso de versões futuras, e não como funcionalidade disponível, o que caracteriza o não atendimento ao item 7.1.3-28.

Service of type LoadBalancer with IPAM for on-prem Kubernetes Cluster (Future versions of TKC)

For Kubernetes hosted in on-premise bare metal Kubernetes clusters, the service of type LoadBalancer could be highly efficient for DevOps and NetOps teams to host their apps and direct the external load balancer Thunder to receive traffic to the VIP that's auto allocated via the IPAM. This function can be used for TCP, UDP and HTTP(s) traffic. With this you are guaranteed consistent cloud load balancing architecture with Thunder ADC and TKC for your on-premise Kubernetes clusters.

Referência: documento 4, seção "KEY Function of TKC"

CONCLUSÃO:

Ficou demonstrado que a solução ofertada **não atende aos itens 7.1.3-25 e 7.1.3-28**.

4. DO NÃO ATENDIMENTO AOS REQUISITOS DE AVALIAÇÃO DE VULNERABILIDADES – ITENS 7.2.4-70 A 7.2.4-80, 7.2.4-86 E 7.2.4-217

ITENS NÃO ATENDIDOS:

- **Item 7.2.4-70:** "Implementar serviço de varredura automáticas de vulnerabilidades de aplicações web;"
- **Item 7.2.4-71:** "Implementar testes de penetração de aplicações totalmente automáticos,

ou seja, sem a necessidade de escrita de scripts, roteiros ou playbooks;"

- **Item 7.2.4-72:** "Implementar identificação, navegação, varredura e testes completos, independentemente da tecnologia da aplicação;"

- **Item 7.2.4-73:** "Implementar relatórios com a vulnerabilidades encontradas, incluindo capturas de tela, vídeos e detalhes técnicos, permitindo uma compreensão completa;"

- **Item 7.2.4-74:** "Fornecer relatórios online e em PDF;"

- **Item 7.2.4-75:** "Informar com detalhes as requisições realizadas que apontaram vulnerabilidades e a resposta da aplicação;"

- **Item 7.2.4-76:** "Permitir o download da resposta da aplicação;"

- **Item 7.2.4-77:** "Permitir configuração de alertas a respecto das varreduras e problemas encontrados;"

- **Item 7.2.4-78:** "Implementar avaliação de exposição de acordo com OWASP Top 10;"

- **Item 7.2.4-79:** "Fornecer orientações de mitigação e correção dos problemas encontrados;"

- **Item 7.2.4-80:** "Permitir inserir notas e observações sobre os problemas encontrados;"

- **Item 7.2.4-86:** "Permitir a configuração de agendas de execução de testes e varreduras periódicos;"

- **Item 7.2.4-217:** "Capacidade de realizar testes de vulnerabilidades para 03 (três) aplicações/mês;"

DOCUMENTO(S) ANALISADO(S):

5. Cloudflare – Changelog: New Vulnerability Scanner for API Shield (09/03/2026)

<https://developers.cloudflare.com/changelog/2026-03-09-vulnerability-scanner>

6. Cloudflare – Dynamic Application Security Testing (DAST)

<https://www.cloudflare.com/lp/security-week/vulnerability-scanner/>

ANÁLISE TÉCNICA:

A documentação oficial da Cloudflare demonstra que seu scanner não atende aos requisitos exigidos, pelos motivos a seguir.

Primeiro, o produto está em fase beta aberta. A Cloudflare anunciou o scanner como Open Beta em março de 2026, restrito a assinantes do API Shield. Um produto em fase de testes não oferece a garantia de funcionamento exigida em uma contratação pública de 60 meses.

New Vulnerability Scanner for API Shield

API Shield

Copy as Markdown | View as Markdown | Agent setup

Introducing Cloudflare's Web and API Vulnerability Scanner (Open Beta)

Cloudflare is launching the **Open Beta of the Web and API Vulnerability Scanner** for all **API Shield** customers. This new, stateful Dynamic Application Security Testing (DAST) platform helps teams proactively find logic flaws in their APIs.

The initial release focuses on detecting Broken Object Level Authorization (BOLA) vulnerabilities by building API call graphs to simulate attacker and owner contexts, then testing these contexts by sending real HTTP requests to your APIs.

Referência: documento 5 Cloudflare.

Em segundo, a varredura se limita a uma única classe de vulnerabilidade de API. Conforme menção do fabricante, a versão inicial foca exclusivamente em vulnerabilidades BOLA (Broken Object Level Authorization). Não há varredura de aplicações web nem teste de penetração abrangente, o que contraria os itens 7.2.4-70, 7.2.4-71, 7.2.4-72 e 7.2.4-217.

The initial release focuses on detecting Broken Object Level Authorization (BOLA) vulnerabilities by building API call graphs to simulate attacker and owner contexts, then testing these contexts by sending real HTTP requests to your APIs.

Referência: documento 5 Cloudflare Changelog, 09/03/2026 / página DAST.

Terceiro, não há avaliação OWASP Top 10 para aplicações web. A própria Cloudflare informa que a varredura dos riscos OWASP Top 10 para aplicações web será disponibilizada futuramente, o que contraria diretamente o item 7.2.4-78.

Dynamic Application Security Testing (DAST)

Scanning for OWASP top ten web application security risks will be available soon in Cloudflare's Application Security platform

Referência: documento 6 Cloudflare – página DAST.

Quarto, não há console nem relatórios. O fabricante informa que o scanner está disponível apenas via API, com a interface no painel prevista para versão futura. Sem interface de console, não há como atender aos itens 7.2.4-73, 7.2.4-74, 7.2.4-75, 7.2.4-76, 7.2.4-77, 7.2.4-79, 7.2.4-80 e 7.2.4-86.

Cloudflare's Web and API vulnerability scanner is the newest addition to Cloudflare Application Security. While Security Center Insights alert via passive configuration and traffic inspection, the new scanner sends HTTP requests, testing APIs and applications for vulnerabilities without relying on existing traffic. Built natively within Cloudflare's global network, the scanner requires no additional infrastructure.

Fill out the form to be notified when we add web application vulnerability focused scanning templates to our new vulnerability scanning capability.

Referência: documento 6 Cloudflare, 09/03/2026.

CONCLUSÃO:

Ficou demonstrado que a solução ofertada **não atende aos itens 7.2.4-70 a 7.2.4-80, 7.2.4-86 e 7.2.4-217.**

5. DO NÃO ATENDIMENTO AO REQUISITO DE EXPORTAÇÃO DE EVENTOS – ITEM 7.2.4-175

ITEM NÃO ATENDIDO:

- Item 7.2.4-175: "Permitir a exportação para, pelo menos, os seguintes sistemas: Kafka, Splunk, Datadog, Azure, Amazon, QRadar e servidores HTTPS genéricos;"

DOCUMENTO(S) ANALISADO(S):

7. Cloudflare – Logpush: Enable destinations

<https://developers.cloudflare.com/logs/logpush/logpush-job/enable-destinations>

ANÁLISE TÉCNICA:

A documentação oficial do serviço de exportação de logs da Cloudflare (Logpush) relaciona como destinos habilitáveis: Cloudflare R2, destino HTTP, Amazon S3, endpoints compatíveis com S3, Datadog, Elastic, Google Cloud Storage, Google BigQuery, Microsoft Azure, New Relic, SentinelOne, Splunk, Sumo Logic, Amazon Kinesis, IBM QRadar e IBM Cloud Logs.

Enable destinations

🕒 Last updated Apr 23, 2026 | 📄 Copy as Markdown | 📖 View as Markdown | 🛠 Agent setup

Enable pushing logs to your storage service, SIEM solution, or log management provider.

Note

Note that you will need to allowlist IP addresses to accept incoming Cloudflare Logpush traffic. Refer to [Cloudflare IPs](#) for the complete list of IPs. If you prefer to have a dedicated IP, you can use dedicated [Dedicated Egress IPs for Cloudflare Logpush](#).

- [Enable Cloudflare R2](#)
- [Enable Cloudflare Pipelines](#)
- [Enable HTTP destination](#)
- [Enable Amazon S3](#)
- [Enable S3-compatible endpoints](#)
- [Enable Datadog](#)
- [Enable Elastic](#)
- [Enable Google Cloud Storage](#)
- [Enable Google BigQuery](#)
- [Enable Microsoft Azure](#)
- [Enable New Relic](#)
- [Enable SentinelOne](#)
- [Enable Splunk](#)
- [Enable Sumo Logic](#)
- [Enable Amazon Kinesis](#)
- [Enable IBM QRadar](#)
- [Enable IBM Cloud Logs](#)
- [Enable other providers](#)
- [Third-party integrations](#)
- [Dedicated Egress IP for Logpush](#)

Referência: documento 7 – Logpush: Enable destinations.

O Kafka, exigido nominalmente no item 7.2.4-175, **não consta** entre os destinos suportados.

CONCLUSÃO:

Ficou demonstrado que a solução ofertada **não atende ao item 7.2.4-175**.

6. CONCLUSÃO FINAL DE RECOMENDAÇÃO

Diante das constatações apontadas neste Parecer Técnico, oriundas da análise minuciosa da documentação apresentada pela empresa THS Tecnologia em sede de diligência, conclui-se que a proposta ofertada **NÃO ATENDE** a requisitos técnicos essenciais estipulados no Termo de Referência (SEI nº 74267331).

A diligência, instaurada com fulcro no Art. 59, § 2º da Lei nº 14.133/2021, objetivou sanear dúvidas quanto às especificações técnicas dos equipamentos e serviços propostos. Contudo, os documentos oficiais dos fabricantes (A10 Networks e Cloudflare) fornecidos pela própria licitante atestaram a incapacidade da solução ofertada de cumprir com especificações mandatórias, notadamente referentes ao throughput real exigido para WAF, à arquitetura dedicada demandada, e à oferta de um pacote Cloudflare genérico em oposição aos requisitos avançados do Termo de Referência. A indefinição do licenciamento na proposta comercial agrava o quadro, ferindo o julgamento objetivo.

Desta forma, a proposta apresenta vícios insanáveis em seu escopo técnico e de formulação, impossibilitando sua aceitação sem grave risco à segurança, performance e gerenciamento da infraestrutura tecnológica pretendida por esta Secretaria, e em clara afronta à Lei de Licitações.

Recomendação

Com base no exposto, este corpo técnico sugere a **DESCCLASSIFICAÇÃO** da proposta apresentada pela empresa THS Tecnologia, Informação e Comunicação LTDA, por não atender aos requisitos técnicos exigidos no Edital e seus anexos.

Recomenda-se, por conseguinte, o regular prosseguimento do certame, com a convocação das licitantes remanescentes, na ordem de classificação, para negociação e posterior análise de habilitação e proposta, em estrita observância aos ditames da Lei nº 14.133/2021.



Documento assinado eletronicamente por **GILSON NEDISON FERREIRA DE SOUZA**, **Gerente.**, em 28/09/2026, às 12:42, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do [Decreto nº 21.794, de 5 Abril de 2017.](#)



Documento assinado eletronicamente por **Plinio Jefferson Bentes dos Santos**, **Coordenador(a)**, em 28/09/2026, às 12:42, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do [Decreto nº 21.794, de 5 Abril de 2017.](#)



A autenticidade deste documento pode ser conferida no site [portal do SEI](#), informando o código verificador **77015797** e o código CRC **7731AF64**.

Referência: Caso responda este Parecer, indicar expressamente o Processo nº 0029.003939/2025-74

SEI nº 77015797