

CONCURSO PÚBLICO COM PUBLICAÇÃO DE ANÚNCIO EM JOUE Nº 29/AT/2025

CADERNO DE ENCARGOS

Aquisição do suporte das plataformas de monitorização, salvaguarda e distribuição de tráfego da rede de visibilidade

Cláusula 1.^a

Objeto

1 - O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objecto a aquisição do suporte das plataformas de monitorização, salvaguarda e distribuição de tráfego da rede de visibilidade do datacenter (DC) da Autoridade Tributária e Aduaneira (AT), de acordo com as seguintes especificações técnicas:

Descrição do bem	Quantidade
Suporte para as 4 licenças Omipeek Savvius Enterprise que se encontram instaladas na AT	1
Equipamentos agregadores de tráfego (de Packet Brokers) com licenciamento perpétuo	2
Equipamento distribuidor de tráfego (de Packet Brokers) com licenciamento perpétuo	1
Plataforma de recolha e armazenamento do tráfego	1

2 - Todos os componentes dos bens estão descritos nas especificações técnicas da parte II do presente caderno de encargos e deverão ter licenciamento perpétuo e suporte do fabricante por 3 anos.

Cláusula 2.^a

Preço Base

O preço máximo que a entidade adjudicante se dispõe a pagar pelos bens e serviços de suporte é de € 667.039,00 (Seiscentos e sessenta e sete mil e trinta e nove euros), a que acresce o IVA à taxa legal em vigor.

Cláusula 3.^a

Prazo de execução

1 - O prazo para a entrega do equipamento e prestação dos serviços de instalação não poderá exceder 60 dias a contar da data de início de produção de efeitos do contrato.

2 - O prazo de vigência do contrato a celebrar é de três anos, a contar da data do início de produção de efeitos do contrato.

Cláusula 4.^a

Local do fornecimento

A instalação da infraestrutura de monitorização deve ser entregue nos dois Datacenter da AT, Edifício Satélite, sito na Avenida Eng.º Duarte Pacheco, n.º 28 – 1099-013 Lisboa e Datacenter do Porto, sito na Rua Diniz Jacinto, 4350-059 Porto.

Cláusula 5.^a

Sigilo e confidencialidade

1. O Adjudicatário obriga-se a guardar sigilo e confidencialidade sobre todos os assuntos constantes do objeto do contrato e a tratar como confidencial toda a informação e documentação, técnica e não técnica, comercial ou outra, ou qualquer assunto que no seu âmbito esteja em desenvolvimento ou colaboração, de que possa ter conhecimento e a que tenha acesso, sendo esta obrigação extensível aos seus agentes, funcionários, colaboradores ou terceiros que as mesmas envolvam.
2. A informação e a documentação cobertas pelo dever de sigilo e confidencialidade não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta ou exclusivamente à execução do contrato.
3. As partes só podem divulgar informações referidas no número anterior na medida em que tal seja estritamente necessário à execução do contrato, mediante autorização da parte que as haja prestado e da AT, se diferente, ou do estritamente necessário ao exercício do direito de defesa em processo contencioso.
4. No caso previsto no número anterior, as partes devem garantir, em reciprocidade e em condições satisfatórias, a assunção, por escrito, de idêntico compromisso de confidencialidade pelos terceiros que acedam às informações abrangidas pelo dever de confidencialidade.
5. As partes devem ainda limitar o acesso às informações confidenciais aos seus quadros e funcionários que a elas tenham de recorrer para a correta execução do contrato, assegurando que os mesmos são obrigados a manter essa confidencialidade.
6. São suscetíveis de serem consideradas informações confidenciais, sem prejuízo de outras que as partes decidam qualificar como tal, as que, a serem divulgadas, possam causar danos a qualquer das partes ou a terceiros, ou perturbar o normal desenvolvimento dos trabalhos da prestação de serviços objeto deste convite.

7. Os deveres referidos nos números anteriores abrangem igualmente as entidades subcontratadas pelo adjudicatário e a equipa técnica a afetar à presente prestação de serviços.
8. Exclui-se do dever de sigilo previsto a informação e a documentação que forem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 6.^a

Proteção de dados

1. As partes comprometem-se a cumprir o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), a Lei n.º 58/2019, de 8 de agosto, e demais legislação de proteção de dados pessoais aplicável.
2. No caso de o Adjudicatário / Segundo Outorgante tratar dados pessoais no âmbito do presente contrato, fica obrigado a tratar os dados exclusivamente na medida do estritamente necessário para integral, pontual e adequada prossecução dos fins constantes do contrato, e por conta e de acordo com as instruções do Adjudicante / Primeiro Outorgante, devendo cumprir rigorosamente as instruções relativas ao acesso, registo, transmissão ou qualquer outra operação e meio de tratamento de dados pessoais.
3. O Adjudicatário / Segundo Outorgante compromete-se ao seguinte:
 - a) Tratar os dados pessoais de forma lícita e com respeito pelo princípio da boa-fé, utilizando-os exclusivamente para as finalidades a que se reporta o contrato, não podendo ser posteriormente tratados de forma incompatível com tais finalidades;
 - b) Implementar as medidas técnicas e organizativas adequadas ao objeto e à natureza do tratamento de dados, assim como ao tipo de dados pessoais e ao tipo de categorias de titulares de dados;
 - c) Implementar as medidas de segurança necessárias para proteger os dados contra destruição acidental ou ilícita, perda acidental, alterações, difusão ou acesso não autorizados, e contra qualquer outra forma de tratamento ilícito dos dados pessoais;
 - d) Assegurar que todos os seus trabalhadores e colaboradores estão vinculados a um compromisso de confidencialidade específico para tratamento de dados no âmbito do presente contrato;

- e) Não recorrer a subcontratantes sem a autorização expressa e por escrito do Adjudicante / Primeiro Outorgante;
 - f) Não proceder a transferências internacionais de dados pessoais, exceto se tal for instrução do Adjudicante / Primeiro Outorgante;
 - g) Prestar assistência e colaboração nos casos em que seja obrigatória uma avaliação de impacto sobre a proteção de dados;
 - h) Prestar assistência e colaboração em caso de violações de dados pessoais;
 - i) Disponibilizar toda a informação pertinente no âmbito do presente contrato e facilitar auditorias e inspeções por parte do Adjudicante / Primeiro Outorgante;
 - j) Comunicar de imediato ao Adjudicante / Primeiro Outorgante quaisquer reclamações ou questões colocadas pelos titulares dos dados pessoais.
4. O Adjudicatário / Segundo Outorgante obriga-se a manter os dados pessoais estritamente confidenciais, sendo responsável pela utilização dos dados pessoais por parte dos respetivos trabalhadores e colaboradores.
5. O Adjudicatário / Segundo Outorgante não pode proceder à reprodução, gravação, cópia ou divulgação dos dados pessoais para outros fins que não constem do contrato.
6. O Adjudicatário / Segundo Outorgante é responsável por qualquer violação de dados pessoais, incluindo a perda ou modificação, ocorrida no âmbito da execução do contrato por causas que lhe sejam imputáveis, ficando obrigado a adotar as medidas que forem necessárias com vista à mitigação da violação sem quaisquer custos adicionais para o Adjudicante / Primeiro Outorgante.
7. O Adjudicatário / Segundo Outorgante obriga-se a ressarcir o Adjudicante / Primeiro Outorgante por todos os prejuízos em que esta venha a incorrer em virtude da utilização ilegal e/ou ilícita dos dados pessoais objeto deste contrato, nomeadamente por indemnizações e despesas em que tenha incorrido na sequência de reclamações ou processos propostos pelos titulares dos dados, bem como, por taxas, coimas e multas que tenha de pagar.

Cláusula 7.^a

Preço contratual e formas de pagamento

1. As quantias devidas para pagamento dos bens e serviços devem ser pagas no prazo de 30 dias a contar da data de receção das faturas, considerando-se vencida a

respetiva obrigação com a emissão de declaração de aceitação, aprovação ou conformidade dos bens/serviços objeto da respetiva fatura.

2. O preço contratual será pago em três prestações anuais, no início de cada ano de vigência do contrato. A fatura relativa ao pagamento da primeira anuidade só pode ser emitida após a emissão de declaração de aceitação, aprovação ou conformidade dos bens/serviços, objeto da fatura. As faturas relativas ao pagamento da segunda e terceira anuidades só podem ser emitidas após o vencimento da obrigação respetiva, a qual ocorre, respetivamente, 12 meses e 24 meses após a data de assinatura do contrato.

Cláusula 8.^a

Força maior

1 - Não podem ser impostas penalidades ao prestador dos serviços, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias, que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.

2 - Constituem motivos de força maior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo e motins e determinações governamentais ou administrativas injuntivas.

3 - A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.

4 - A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 9.^a

Resolução do contrato

1 - O contrato pode ser resolvido por qualquer das partes em caso de incumprimento definitivo, grave ou reiterado, e culposos por uma das Partes das obrigações por si assumidas no contrato, nos termos gerais de Direito, sem prejuízo das correspondentes indemnizações legais a que houver lugar.

2 - Para efeitos do disposto no número anterior, a Parte não culposa comunicará por escrito a ocorrência da situação de incumprimento suscetível de gerar resolução contratual, concedendo à contraparte um prazo não inferior a 30 dias para que aquela reponha a situação de incumprimento, sem o que, o incumprimento se tornará definitivo e determinará a resolução contratual, nos demais termos gerais de direito.

3 - O contrato pode também ser resolvido através da AT caso se verifique alguma das seguintes situações, as quais são desde já entendidas como situações de incumprimento grave e culposos por parte do prestador dos serviços:

- a) Quando se verificar reiterada inobservância das disposições do contrato ou má fé do prestador dos serviços;
- b) Prestação de falsas declarações;
- c) Estado de falência ou insolvência;
- d) Cessaçã da atividade;
- e) Condenaçã, por sentençã transitada em julgado, por infraçã que afete a idoneidade profissional do prestador dos serviços e desde que não tenha ocorrido reabilitaçã judicial.

4 - O direito de resolução referido no número anterior exerce-se mediante declaraçã escrita enviada ao prestador dos serviços nos termos do n.º 2 desta cláusula.

Cláusula 10.^a

Execuçã da cauçã

1. A cauçã prestada para bom e pontual cumprimento das obrigaçõs decorrentes do contrato, nos termos do convite, pode ser executada pela AT, sem necessidade de prévia decisã judicial ou arbitral, para satisfaçã de quaisquer créditos resultantes de mora, cumprimento defeituoso, incumprimento definitivo pelo fornecedor das obrigaçõs contratuais ou legais, incluindo o pagamento de penalidades, ou para quaisquer outros efeitos especificamente previstos no contrato ou na lei.

2. A cauçã a que se referem os números anteriores é liberada nos termos do artigo 295.º do Código dos Contratos Públicos.

Cláusula 11.^a

Comunicaçõs e notificaçõs

1 - Sem prejuízo de poderem ser acordadas outras regras quanto às notificaçõs e comunicaçõs entre as partes do contrato, estas devem ser dirigidas, nos termos do

Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.

2 - Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

PARTE II - CLÁUSULAS TÉCNICAS

1. Suporte de 4 licenças da AT OmniPeek LiveAction Enterprise ou substituição por equivalente devendo cumprir no mínimo os seguintes requisitos:

- a. A solução deverá integrar com o Wireshark, através de ficheiros
- b. Deverá ter a capacidade de analisar em tempo real e de analisar captura baseadas em ficheiros;
- c. Capturar e dissecar wireless 802.11n e 802.11ac de APs Cisco, Aruba, etc.
- d. Classificar o tráfego em Layer7
- e. Monitorizar protocolos, performance aplicacional apresentando os dados em dashboards de alto nível
- f. Capturar em simultâneo em várias placas rede
- g. Deverá ter módulo de análise, reportando indicadores relacionados com:
 - i. Protocolos:
 1. Utilização;
 2. Desconformidade;
 3. Latência
 - ii. Desempenho aplicacional
 - iii. Segurança
- h. Correlacionar capturas efetuadas em localizações distintas, apresentando os resultados de forma integrada
- i. Monitorizar voz e vídeo em tempo real, apresentando indicadores compreensivos de sinalização e de qualidade de serviço
- j. Desencriptar WEP, WPA/PSK, WPA2 e SSL
- k. Alterar filtros de captura em voo
- l. Identificar e discriminar os indicadores relevantes numa aplicação WEB:
 - i. Páginas
 - ii. Respostas
 - iii. Servidor
 - iv. Cliente
- m. Deverá ter dissecação e análise dos principais protocolos de rede incluindo sqlnet

2. Dois equipamentos agregadores Ixia E100S ou equivalentes com funcionalidade inline e fabric controller ou equivalente, devendo cumprir os seguintes requisitos por equipamento:
- a) Deverá ter fontes de alimentação redundantes
 - b) Cada equipamento deverá ter 32 portas licenciadas de 100Gbits
 - c) Deverá ter a capacidade de unificar o control-plane de gestão funcionado como se fosse um único equipamento
 - d) Deverá ter a capacidade de receber o tráfego encapsulado;
 - e) Implementar encadeamento de ativos (IPSS,Firewalls,etc) nos circuitos principais da AT com a capacidade de selecionar os caminhos de forma discricionária programável , baseada nas regras do negocio e dependente do estado operacional dos equipamentos conexos;
 - f) Implementar filtragem e entrega de pacotes sobre as coletas sem a supressão de pacotes originais quando existe interceção de contextos de captura (“overlapping”), entre portas, vlans e endereçamento. Ou seja, o equipamento deve ter a capacidade de processar e entregar os pacotes em várias políticas de forma independente, sem haver qualquer interferência entre elas.
 - g) Deverá ter a capacidade de comutação igual ou superior ao ritmo de transmissão agregado de todas as portas;
 - h) Deverá vir acompanhados com:
 - i. 20 transceivers óticos QSFP-PLUS-SR4-XCVR MPO/MPT
 - ii. 10 transceivers óticos QSFP28-SR4-XCVR MPO/MPT
 - iii. 30 cabos de breakout CKT-MTP-4LC-50-OM4
 - iv. 30x4 adaptadores LC fêmea-fêmea
 - v. 4 Twinax Cable 100G QSFP28 Active Direct Attach Copper - 3mt
 - vi. 4 40G QSFP+ Passive Direct Attach Cable 3mt
 - vii. 8 10G SFP+ Passive Direct Attach Copper Twinax Cable 3mt

3. Um equipamento distribuidor IXIA Vision 400 com PactekStack ou equivalente, devendo cumprir os seguintes requisitos:
- a) Ter fontes de alimentação redundantes
 - b) A capacidade de comutação deve ser igual ou superior ao ritmo de transmissão agregado de todas as portas
 - c) Ter a capacidade de remover duplicados de pelo menos 400 Gibits de tráfego de rede em tempo real (packet deduplication) tanto na receção, nos filtros ou na entrega de tráfego
 - d) Ter as funcionalidades de duplicação, trimming, stripping (PacketStack) disponível em todas as portas
 - e) Implementar filtragem e entrega de pacotes sobre as coletas sem a supressão de pacotes originais quando existe interceção de contextos de captura (“overlapping”), entre portas, vlans e endereçamento. Ou seja, o equipamento deve ter a capacidade de processar e entregar os pacotes em várias políticas de forma independente, sem haver qualquer interferência entre elas.
 - f) Suportar as seguintes características:
 - i. Proteção contra picos de tráfego através do uso de buffer de memória;
 - ii. TimeStamping
 - iii. Masking
 - iv. Timestamping
 - v. Trimming
 - vi. Trailer
 - vii. Tunneling sobre GRE
 - viii. Header striping
 - g) Deve ter 24 Portas SFP56(10/25/50) licenciadas
 - h) Deve ter 16 Portas QSFP56DD - 2 licenciadas a 400G e 14 licenciadas a 100G
 - i) Deve vir acompanhado com:
 - i. 4 transceivers óticos 100G QSFP28-SR4-XCVR MPT

- ii. 10 transceivers óticos QSFP-PLUS-SR4-XCVR MPT
 - iii. 14 cabos de breakout CKT-MTP-4LC-50-OM4
 - iv. 14x4 adaptadores LC Femea-Femea
 - v. 8 transceivers óticos SFP56
 - vi. 4 transceivers óticos SFP28
 - vii. 4 Twinax Cable 100G QSFP28 Active Direct Attach Copper – 1m
4. Uma plataforma de salvaguarda de tráfego Livewire Powercore Gen 2 240T com capacidade de geração e exportação de indicadores de comunicações para o splunk ou equivalente, devendo cumprir os seguintes requisitos:
- a) Deverá ter a capacidade de armazenar 240TB de tráfego
 - b) Deverá ter mecanismos de compressão no hardware que permitam expandir a capacidade da alínea anterior para um valor de 720TB (assumindo um fator de compressão de 1:3)
 - c) Deverá ter no mínimo 256GB de memória
 - d) Deverá ter a capacidade mínima de escrita em disco de 25Gbps e 75 efetivos
 - e) Deverá ter a capacidade mínima de análise para telemetria de 60 Gbps
 - f) Deverá ter duas interfaces de captura a 100Gbit/s em placa de rede programável com FPGAs com buffer de memória para acomodar burst, ter capacidade de fazer a filtragem no hardware e apresentar no Sistema operativo o tráfego selecionado em placas de rede virtualizadas para atribuí-las de forma transparente e diferenciada aos processos de análise respetivos;
 - g) Deverá permitir a alteração dos filtros da alínea anterior em voo
 - h) Analisar o tráfego e reportar:
 - i. Utilização dos protocolos
 - ii. Desconformidades e anomalias
 - iii. Indicadores com thresholds programáveis:
 - a) Voz:
 - i. Sinalização:

- i. H225
 - ii. H245
 - iii. SIP
- ii. RTP:
 - i. Jitter medido
 - ii. Jitter reportado
 - iii. Packet loss medido
 - iv. Packet loss reportado
 - v. Falta de QoS
 - vi. Low MOS
 - vii. Low R factor
- b) Cliente/servidor:
 - i. Baixo ritmo de transmissão IN
 - ii. Baixo ritmo de transmissão OUT
 - iii. Cliente não responsivo
 - iv. Tráfego num sentido
 - v. Slow server response
- c) Aplicação:
 - i. DHCP:
 - i. Request Storm
 - ii. Multiple response
 - iii. Request rejected
 - ii. DNS:
 - i. Slow response time
 - ii. Dominio inexistente
 - iii. HTTP:
 - i. Client error
 - ii. Server error
 - iii. Slow Response
 - iv. Not Found
 - iv. Oracle:
 - i. Logon denied
 - ii. Slow response
 - iii. Conexão negada

- v. Kerberos:
 - i. Request rejected
- vi. LDAP:
 - i. Slow response
- vii. SMB:
 - i. Excessivos loops transacionais
 - ii. Access denied
- d) Transporte:
 - i. TCP:
 - i. Ligações:
 - a) Recusadas
 - b) Perdidas
 - c) Reset
 - d) Inativas
 - e) Tentativas Repetidas
 - ii. Retransmissões:
 - a) Contador
 - b) Demasiadas
 - c) Fast by Ack
 - d) Fast by time
 - iii. Janelas:
 - a) Presa
 - b) Zero
 - iv. ACK
 - v. Duplicado
 - vi. Selective SACK
- e) Rede:
 - i. IP:
 - i. Local routing
 - ii. Checksum invalido
 - iii. Pacote duplicado
 - iv. Falta de fragmento
 - v. Tamanho inconsistente
 - ii. ICMP:

- i. Network unreachable
 - ii. Host unreachable
 - iii. Protocol unreachable
 - iv. Host redirect
 - v. TTL exceeded
 - iii. IPSEC ESP fora de sequência
- f) Data Link:
 - i. 802.1X ataque de dicionário
 - ii. Storm:
 - i. ARP
 - ii. BroadCast
 - iii. Multicast
 - iii. Alteração de topologia STP
 - iv. Falha de autenticação EAP
- iv. Desempenho aplicacional
- v. Indicadores de segurança
- vi. Monitorizar a voz e vídeo em tempo real, apresentando indicadores compreensivos de sinalização e de qualidade de serviço
- vii. Identificar e discriminar os indicadores relevantes numa aplicação WEB:
 - a) Páginas
 - b) Respostas
 - c) Servidor
 - d) Cliente
- i) Deve ter dissecação e análise dos principais protocolos de rede incluindo sqlnet
- j) Deve ter a capacidade de exportar todos os indicadores anteriores para o splunk
- k) Deve ter a capacidade de exportar a informação sobre os fluxos de comunicações para o splunk, nomeadamente:
 - i. Peers:
 - a) Cliente
 - b) Servidor
 - ii. DPI:
 - a) Protocolo
 - b) Aplicação

- iii. País do IP de cliente
- iv. Número de indicadores relevantes no fluxo
- v. Bytes IN/OUT
- vi. 3Way Handshake
- vii. Latência por fluxo:
 - a) Melhor
 - b) Média
 - c) Pior
- viii. Ritmos de transmissão por fluxo IN/OUT:
 - a) Melhor
 - b) Médio
 - c) Pior