Procedimento n.º CP/3/2025

Contrato nº CP/03/2025

AQUISIÇÃO DE SERVIÇOS PARA A INFRAESTRUTURA DE REDE E SEGURANÇA PARA O MECANISMO NACIONAL ANTICORRUPÇÃO (MENAC)

PARTE I - FACTOS REFERENCIAIS DE BASE E LEGITIMADORES DO CONTRATO

Intervenientes no acto:

Entre o **Mecanismo Nacional Anticorrupção (MENAC)**, adiante designado de contraente público ou primeiro outorgante, pessoa colectiva n. º 517 091 178, com sede nas Escadinhas de S. Crispim, n.º 7, 1149-049, Lisboa, representado neste acto pelo Secretário-Geral do MENAC, Jorge Duque Lobato, com poderes para a prática deste acto, como Primeiro Outorgante, nos termos do Despacho 4489/2023, de 14 de Março, publicado em Diário da República n.º 73, 2.ª série, de 13 de Abril de 2023 e a empresa **Inetum España, S.A. - Sucursal em Portugal**, adiante designado de co-contratante ou segundo outorgante, pessoa colectiva nº 980 079 659, com sede na Rua Afonso Praça, n.º 30, 3.º, 1495 064 Algés, neste ato representada por Pedro Miguel Soares Gomes dos Santos, titular do cartão do cidadão n.º [redacted], na qualidade de representante legal, os quais têm poderes para outorgar o presente contrato, conforme documentos comprovativos que exibiram, como Segundo Outorgante é celebrado o presente contrato.

DESIGNAÇÃO DA AQUISIÇÃO:

AQUISIÇÃO DE SERVIÇOS PARA A INFRAESTRUTURA DE REDE E SEGURANÇA PARA O MECANISMO NACIONAL ANTICORRUPÇÃO (MENAC)

VALOR:

O preço a pagar pelo fornecimento dos serviços objecto do contrato é de **78 981,42 €** **(Setenta e oito mil novecentos e oitenta e um euros e quarenta e dois cêntimos)**, a que acresce o IVA, à taxa legal em vigor.

IDENTIFICAÇÃO E MODALIDADE DO PROCEDIMENTO DE CONTRATAÇÃO PÚBLICA ADOPTADO:

Procedimento por Concurso Público, sem publicação no JOUE, CP/03/2025, para a aquisição de serviços para a infraestrutura de rede e segurança para o Mecanismo Nacional Anticorrupção (MENAC), ao abrigo da alínea b) do n.º 1 do artigo 20.º do Código dos Contratos Públicos (CCP), aprovado pelo decreto-lei n.º 18/2008, de 29 de janeiro, na sua actual redacção.

DESPACHO QUE AUTORIZOU A ABERTURA DO PROCEDIMENTO:

Despacho de 12 de março de 2025, do Sr. Secretário-Geral do MENAC, Jorge Duque Lobato, exarado na informação n.º 55/2025, de 10 de março.

DESPACHO QUE AUTORIZOU A ADJUDICAÇÃO E A CELEBRAÇÃO DO CONTRATO:

Despacho de 26 de março de 2025, do Sr. Secretário-Geral do MENAC, Jorge Duque Lobato, exarado na informação n.º 31/2025, de 26 de março.

DESPACHO DE APROVAÇÃO DA MINUTA:

Despacho de 26 de março de 2025, do Sr. Secretário-Geral do MENAC, Jorge Duque Lobato, exarado na informação n.º 31/2025, de 26 de março de 2025.

PARTE II - CLÁUSULAS CONTRATUAIS

CAPÍTULO I - DISPOSIÇÕES GERAIS

Cláusula 1.ª Objecto

§ O presente contrato tem por objecto a aquisição de serviços para a infraestrutura de rede e segurança para o Mecanismo Nacional Anticorrupção (MENAC)

Cláusula 2.ª Contrato

1. O contrato é reduzido a escrito, nos termos do n.º 1 do artigo 94.º do CCP.

2. Fazem parte integrante do contrato os seguintes documentos:

   a) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;

   b) Os esclarecimentos e as rectificações relativos ao caderno de encargos;

   c) O Caderno de Encargos;

   d) A proposta adjudicada;

   e) Os esclarecimentos sobre a proposta adjudicada prestados pelo co-contratante.

3. Em caso de divergência entre os documentos referidos no n.º 2, a prevalência é determinada pela ordem que nele se dispõe.

4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código

dos Contratos Públicos e aceites pelo co-contratante nos termos do disposto no artigo 101.º desse mesmo diploma legal.

Cláusula 3.ª – Prazo

1. A prestação objecto do contrato, terá uma duração de 2 meses e decorrerá entre **15 de abril** e **15 de junho de 2025**, de forma continua e de acordo com o Caderno de Encargos, nomeadamente quanto às cláusulas técnicas, sem prejuízo das obrigações acessórias que devam perdurar além da cessão da vigência do contrato.

CAPÍTULO II OBRIGAÇÕES CONTRATUAIS

Secção I - Obrigações do co-contratante

Cláusula 4.ª - Obrigações Gerais do co-contratante

1. Sem prejuízo de outras obrigações previstas na legislação aplicável e no Caderno de Encargos decorrem para o co-contratante as obrigações a seguir indicadas:

   a) Disponibilização, instalação, configuração e manutenção de uma solução PaaS – Cloud Pública e de uma infraestrutura de rede e segurança, conforme descrito nas cláusulas técnicas (Anexo I) do presente Caderno de Encargos;

   b) Manutenção das condições do fornecimento dos bens e serviços descritas nas cláusulas técnicas do caderno de encargos;

   c) Execução do objeto contratual de forma profissional e competente, utilizando os conhecimentos técnicos, o *know-how*, a diligência, o zelo e a pontualidade próprios das melhores práticas;

   d) Para a execução dos serviços técnicos, o Adjudicatário fica obrigado a

disponibilizar os recursos necessários, com os conhecimentos técnicos adequados à função;

e) Comunicação antecipada dos factos que tornem total ou parcialmente impossível a prestação do serviço ou o cumprimento de qualquer outra obrigação;

f) Prestação de forma correcta e fidedigna das informações referentes às condições em que é efectuada a prestação do serviço, bem como prestação de todos os esclarecimentos que sejam solicitados;

g) Comunicar qualquer facto que ocorra durante o período de vigência do contrato e que altere, designadamente, a denominação social os seus representantes legais, a sua situação jurídica e comercial;

h) Obrigação de substituição de qualquer dos elementos da equipa técnica a afectar à execução dos serviços;

i) Comunicar à Entidade Adjudicante a identificação do responsável designado para a gestão do contrato, nomeadamente, para efeitos de comunicações e demais situações necessárias, o qual deverá estar definido no momento da assinatura do contrato, bem como quaisquer alterações quanto ao gestor indicado.

a) Sempre que ocorra um caso de força maior, devidamente comprovado e que implique a suspensão do serviço, deve o co-contratante, logo que tenha conhecimento, notificar o MENAC.

2. Quaisquer anomalias na execução do contrato, imputáveis ao co-contratante, fica este obrigado a suportar os custos inerentes à reposição das condições de do serviço objecto do contrato, anteriores à ocorrência da(s) anomalia(s).

Cláusula 5ª - Meios Humanos e Materiais

1. O co-contratante obriga-se a recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução do contrato;

2. São da exclusiva responsabilidade do co-contratante as obrigações relativas ao pessoal por si utilizado na execução dos trabalhos, à sua aptidão profissional, à disciplina, à sua conduta, ao seu comportamento moral e à sua responsabilidade civil;

3. Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato;

4. São da responsabilidade do co-contratante quaisquer encargos decorrentes da obtenção ou utilização, no âmbito do contrato, de patentes, licenças ou marcas registadas.

Cláusula 6.ª – Sigilo

1. O co-contratante deve guardar sigilo sobre toda a informação e documentação, relativa ao MENAC, que lhe seja fornecida ou a que tenha acesso, no âmbito da execução do contrato, perdurando o dever de sigilo até dois anos após a cessação do contrato seja qual for a causa desta.

2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objecto de qualquer uso ou modo de aproveitamento que não o destinado directa e exclusivamente à execução do contrato.

Cláusula 7ª – Protecção de dados

§ Não obstante do expressamente previsto, sempre que haja acesso a dados pessoais, por inerência da execução do contrato, por parte do co-

contratante e respectivos colaboradores, é aplicável o Regime Jurídico da Protecção de Dados (RJPD) regulado pela Lei n.º 58/2019, de 8 de Agosto, bem como demais legislação extravagante, que a esta matéria importe. À violação destas disposições aplicar- se-ão as sanções previstas nos mesmos preceitos legais.

Secção II - Obrigações do Contratante

Cláusula 8ª - Gestor do Contrato

§ Nos termos e para os efeitos do artigo 290.º-A do CCP, o MENAC designa para gestor de contrato o Eng. João Carlos Mesquitela, como gestor de contrato, com a função de acompanhar em permanência a execução deste.

Cláusula 9ª - Preço contratual

1. Pela prestação objecto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o MENAC, deve pagar ao co-contratante o preço global de **78 981,42 €** (Setenta e oito mil novecentos e oitenta e um euros e quarenta e dois cêntimos), a que acresce o IVA, à taxa legal em vigor.

2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, incluindo as despesas de alojamento, alimentação e deslocação de meios humanos.

Cláusula 10.ª - Condições de pagamento

1. As quantias devidas pelo MENAC, nos termos da Cláusula 9.ª, serão pagas mensalmente no prazo de 30 dias, após emissão da factura.

2. O pagamento referido do n.º 1, inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante.

3. A emissão da referida factura deverá ser processada após a aceitação dos trabalhos pelo MENAC, com todos os elementos justificativos do total apresentado.

4. As facturas deverão ser enviadas em formato digital para o endereço geral@mec- anticorrupcao.pt ou através do Portal da Factura Electrónica na Administração Pública.

5. Caso as facturas apresentadas não sejam validadas pelo MENAC, porque desconformes com o contrato, este comunicará tal decisão ao co-contratante, o qual deverá apresentar outras em sua substituição, devidamente corrigidas.

6. O pagamento será efectuado por transferência bancária, para o IBAN indicado e mediante entrega de comprovativo, pelo co-contratante.

Cláusula 11.ª - Revisão de preços

§ Os preços contratualizados são fixos e não sujeitos a revisão ou actualização, durante o prazo total de vigência do contrato.

CAPÍTULO III - PENALIDADES E RESOLUÇÃO

Cláusula 12.ª - Força maior

1. Não podem ser impostas penalidades ao co-contratante, nem é havida como incumprimento, a não realização pontual das obrigações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respectiva

realização, alheias à vontade da parte afectada, 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. Consideram-se como motivos de força maior, designadamente, os seguintes:

a) Epidemias supervenientes, greves, conflitos laborais, insurreições ou motins, guerra, invasão e mobilização que originem a suspensão ou interrupções do trabalho;

b) Movimentos sísmicos, incêndios, explosões, inundações e acidentes graves que suspendam ou interrompam o trabalho.

3. Não constituem casos de força maior, designadamente:

a) Circunstâncias que não constituam força maior para os subcontratados do co- contratante, na parte em que intervenham;

b) Greves ou conflitos laborais limitados às sociedades do co-contratante ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;

c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo co- contratante de deveres ou ónus que sobre ele recaiam;

d) Manifestações populares devidas ao incumprimento pelo co-contratante de normas legais;

e) Incêndios ou inundações com origem nas instalações do co-contratante cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;

f) Avarias nos sistemas informáticos ou mecânicos do co-contratante não devidas a sabotagem;

g) Eventos que estejam ou devam estar cobertos por seguros.

4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte, devendo o co-contratante informar, da duração previsível do incumprimento.

5. 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 13.ª - Sanções por incumprimento

1. Sem prejuízo do direito, da entidade adjudicante, de resolução do contrato pelo não cumprimento pontual de obrigações dele emergentes, se o adjudicatário não cumprir, por razões que lhe sejam imputáveis, as condições contratuais assumidas, incorrerá no pagamento da penalidade de 2% (dois por cento) do preço contratual por cada semana de atraso ou situação de incumprimento do contrato.

2. O valor acumulado das sanções eventualmente aplicadas ao abrigo da presente cláusula não pode exceder 20% (vinte por cento) do preço contratual, sem prejuízo do poder de resolução do contrato previsto na cláusula seguinte.

3. Caso seja atingido o limite previsto no número anterior e a entidade adjudicante decida não proceder à resolução do contrato por dela resultar grave dano para o interesse público, aquele limite é elevado para 30% (trinta por cento) do preço contratual.

4. A aplicação das penalidades contratuais não exclui o direito de indemnização por perdas e danos com base na legislação em vigor

5. A cobrança das eventuais sanções em que o adjudicatário incorra poderá ser efectuada, a critério da entidade adjudicante, nomeadamente, por desconto nos pagamentos subsequentes à verificação do facto que tenha dado origem à penalidade.

6. A aplicação das sanções previstas na presente cláusula será objecto de audiência prévia, nos termos previstos no n.º 2 do artigo 308 do CCP.

Cláusula 14.ª - Resolução por parte do MENAC

§ Sem prejuízo de outros fundamentos de resolução previstos na lei, o MENAC pode, nos termos da alínea c), do artigo 330.º e artigo 333.º do CCP, resolver o contrato a título sancionatório, no caso do co-contratante violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.

Cláusula 15.ª - Resolução por parte do co-contratante

§ O co-contratante pode resolver o contrato nos termos dos artigos 332º e 449º do CCP.

CAPÍTULO IV - CAUÇÃO E SEGUROS

Cláusula 16.ª - Seguros

§ O co-contratante deverá estar segurado, através de apólices com cobertura de riscos associados ou que possam advir do cumprimento do contrato, nomeadamente seguro de responsabilidade civil profissional e seguro de acidentes de trabalho, que abranja todos os trabalhadores a prestar serviço no MENAC.

Cláusula 17.ª - Caução

§ Não será exigida a prestação de caução, de acordo com o previsto no n.º 2 do artigo 88.º do Código dos Contratos Públicos.

CAPÍTULO V - RESOLUÇÃO DE LITÍGIOS

Cláusula 18.ª - Foro competente

§ Para resolução de todos os litígios decorrentes do contrato fica estipulada a

competência do Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

CAPÍTULO VI - DISPOSIÇÕES FINAIS

Cláusula 19.ª - Comunicações e notificações

1. Em sede de execução contratual, todas as comunicações entre o MENAC e o co- contratante são efectuadas por escrito e enviadas através de correio registado, ou correio electrónico, para os dados indicados na identificação das partes.

2. Deverá ainda ser estipulado o ponto de contacto e respectivos dados, para assuntos respeitantes a gestão corrente, em conformidade com a alínea g) n.º 1 do artigo 4.º do Caderno de Encargos.

Cláusula 20.ª - Subcontratação e cessão da posição contratual

§ A subcontratação pelo fornecedor e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do Código dos Contratos Públicos.

Cláusula 21.ª - Contagem dos prazos

§ Os prazos previstos no contrato seguem o disposto no artigo 470.º do CCP.

Cláusula 22.ª - Legislação aplicável

§ Em tudo o que não se encontrar especialmente regulado, aplicam-se as disposições constantes do Código dos Contratos Públicos e demais legislação aplicável.

PARTE III - ANOTAÇÕES

O segundo outorgante provou que tem a sua situação contributiva regularizada, relativamente a dívidas por impostos ao Estado Português e por contribuições para a Segurança Social.

O encargo previsto é de 78 981,42 € (setenta e oito mil novecentos e oitenta e um euros e quarenta e dois cêntimos), ao qual acresce IVA à taxa legal em vigor, no montante de 18 165,73 € (dezoito mil cento e sessenta e cinco euros e setenta e três cêntimos), perfazendo um total de 97 147,15 € (noventa e sete mil cento e quarenta e sete euros e quinze cêntimos).

O presente contrato será suportado por conta de verbas inscritas no Orçamento do Mecanismo Nacional Anticorrupção (MENAC), para o ano 2025, a que foi dado o compromisso n.° JK42500051.

O presente contrato vai ser assinado pelos representantes dos outorgantes, de cujo conteúdo tomaram perfeito conhecimento.

O primeiro outorgante:

Assinado por: **JORGE MANUEL DUQUE LOBATO**
Num. de identificação: [redacted]
Data: 2025.04.10 15:43:26+01'00'

O segundo outorgante:

inetum.

Digitally signed by PEDRO MIGUEL SOARES GOMES DOS SANTOS
Date: 2025.04.11 09:45:46 +01'00'

ANEXO I

Requisitos / especificações técnicas dos Equipamentos e Serviços

1. **Solução Segurança – Next Generation Firewall (NGFW) FortiGate 70F**

a) O Mecanismo Nacional Anticorrupção pretende adquirir uma solução de segurança de perímetro de rede composta por uma firewall de próxima geração (NGFW) com funcionalidades de SD-WAN, módulos de IDS/IPS e respectivo licenciamento, bem como a subscrição de funcionalidades de segurança avançada. Adicionalmente, são necessários serviços de implementação, configuração, suporte técnico especializado, actualizações de software e manutenção dos equipamentos, de acordo com as características, requisitos técnicos e condições definidas no presente caderno de especificações técnicas.

b) Pretende-se a aquisição de uma firewall com a funcionalidade de SD-WAN de um fabricante reconhecido pela Gartner como líder no quadrante mágico de Enterprise Wired and Wireless LAN Infrastructure, Network Firewalls, e SD-WAN.

c) A solução deverá incluir um serviço de **suporte técnico premium com uma duração de 3 anos**, abrangendo:

- Assistência Técnica Especializada 24/7: Acesso a suporte técnico contínuo, incluindo ajuda na resolução de problemas e esclarecimento de dúvidas operacionais.
- Substituição Avançada de Hardware: Garantia de substituição rápida de equipamentos em caso de falha de hardware, minimizando tempos de inactividade.
- Actualizações de Firmware e Manutenção Proactiva: Acesso contínuo a actualizações de firmware e software para garantir que a solução mantém um desempenho optimizado e está protegida contra as mais recentes vulnerabilidades.

- Gestão de Incidentes Críticos: Suporte especializado para resposta rápida a incidentes de segurança ou falhas críticas de sistema.

Além disso, a solução deve incluir uma subscrição de Protecção Unificada contra Ameaças (UTP) por 3 anos, englobando:

- Antivírus e Antimalware: Detecção e bloqueio de software malicioso em tempo real.
- Filtragem de Web e Inspecção de Conteúdo: Controlo de acesso a sites e inspecção de conteúdos potencialmente perigosos.
- Sistema de Prevenção e Detecção de Intrusões (IDS/IPS): Monitorização contínua de tráfego para identificar e mitigar ataques de rede.
- Controlo de Aplicações e Gestão de Políticas de Segurança: Definição e aplicação de políticas de segurança para gestão do tráfego de aplicações na rede.
- Protecção Avançada contra Ameaças e Actualizações Diárias: Inclui inteligência contra ameaças emergentes, garantindo uma resposta rápida a novos vectores de ataque.

d) Deverá ser comtemplada, formação para 1 pessoa de forma que a mesma fique com os conhecimentos necessários para administração da solução proposta. A referida formação ter de ser dada directamente pelo fabricante ou por um parceiro devidamente habilitado.

e) A unidade deverá possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

Especificação técnica	Valor
Conectividade	
Interfaces 10/100/1000 RJ45 Aceleradas ASIC	5x GE RJ45
Interface USB Client	1

Interface de Console (RJ45)	1
Desempenho	
Aceleração do tráfego de Firewall, SSL e IPSec por hardware	Hardware dedicado
Aceleração de tráfego NGFW por hardware	Hardware dedicado
Débito firewall (pacotes UDP de 1518 / 512 / 64 bytes)	5 / 5 / 5 Gbps
Latência de firewall (pacotes UDP de 64 bytes)	2.97 µs
Débito firewall (pacotes por segundo)	7.5 Mpps
Sessões TCP concorrentes	700.000
Novas sessões/segundo (TCP)	35.000
Politicas de firewall	5.000
Débito VPN IPSec (pacotes 512 bytes)	4.4 Gbps
Túneis IPsec Gateway-to-Gateway	200
Túneis IPSec cliente remoto	250
Débito VPN SSL	490 Mbps
VPN SSL - Máximo RECOMENDADO de utilizadores simultâneos	200
Débito de inspeção SSL	310 Mbps
Débito de Application Control	990 Mbps
Débito IPS	1 Gbps
Débito NGFW	800 Mbps
Débito Threat Protection	600 Mbps
Domínios Virtuais (por defeito / máximo)	10 / 10
Máximo de FortiAPs controlados (Total / Tunnel Mode)	16/8
Máximo de FortiSwtich controlados	8
Máximo de FortiTokens	500
Licenciamento ilimitado de utilizadores	SIM
Energia e Alimentação	

Alimentação AC	100–240V AC, 50–60 Hz
Consumo de energia médio	7.74 W
Consumo de energia máximo	9.46 W
Dissipação Térmica	52.55 BTU/h
Condições ambientais	
Fanless	SIM
Temperatura de funcionamento	0 - 40 °C
Humidade	10 a 90% sem condensação
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
Certificações	USGv6/IPv6

2. **Solução de rede WI-FI (7 Equipamentos) - FortiAP-221E**

a) O Mecanismo Nacional Anticorrupção pretende adquirir uma solução de rede Wi-Fi composta por 7 equipamentos (AP´s) que inclua pontos de acesso avançados com suporte para as mais recentes tecnologias de conectividade sem fios, garantindo elevada performance, segurança e gestão centralizada da rede. A solução deverá suportar funcionalidades de controlo de acesso, optimização do tráfego, cobertura abrangente e segura, e possibilitar a gestão eficaz de utilizadores e dispositivos. Adicionalmente, são necessários serviços de suporte técnico especializado premium com uma duração de 3 anos, incluindo implementação, configuração, actualizações de software, manutenção contínua dos equipamentos e assistência técnica, conforme as especificações e requisitos definidos no presente caderno de encargos.

b) Deverá ser comtemplada, formação para 1 pessoa de forma que a mesma fique com os conhecimentos necessários para administração da solução

proposta. A referida formação ter de ser dada directamente pelo fabricante ou por um parceiro devidamente habilitado.

c) A unidade deverá possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

Requisitos de Gestão e Operação:

As seguintes funcionalidades deverão ser suportadas:

- O equipamento permite ser configurado através do Controlador de Equipamentos Wi-Fi
- O equipamento permite ser configurado através do sistema de gestão centralizada do Sistema de Segurança
- O equipamento permite funcionar no modo Remote VPN tunnel
- O equipamento permite a descoberta automática de Controladores de Equipamentos Wi-Fi e efectuar o download de configurações para instalações plug-and-play
- O equipamento suporta SNMP
- Possibilidade de ser gerido através de uma consola "single pane of glass"
- O equipamento deverá permitir a integração de uma plataforma centralizada
- O equipamento deverá permitir ser gerido via cloud
- Possibilidade de visualizar e localizar o equipamento através de um mapa
- Possibilidade de gerar relatórios de todos os eventos e performance através de uma plataforma centralizada
- Possibilidade de monitorizar o estado do equipamento a partir de uma plataforma centralizada

Requisitos de Segurança:

- O equipamento permite efectuar o controlo de acesso por autenticação WEP, WPA-PSK, WPA-TKIP, WPA2-AES, 802.11i, 802.1X (EAP-TLS, EAP-TTLS, PEAP, LEAP, EAP-FAST, EAP-SIM, EAPAKA, and EAP-MD5)
- O equipamento permite efectuar o controlo de acesso por autenticação por 802.1X e através de um portal (captive portal), sobre uma base de dados local, RADIUS e Active Directory
- O equipamento permite controlo de acesso RADIUS por utilizador e ESSID, através de filtragem MAC

Requisitos Wireless:

- O equipamento implementa as normas IEEE 802.11 a/b/g/n/ac
- O equipamento implementa MIMO 2x2 (dual stream)
- O equipamento deverá permitir débitos optimizados através de Automatic Radio Resource Provisioning (ARRP)

Certificações

O equipamento deverá ter as seguintes certificações:

- O equipamento terá que ter a certificação DFS (dynamic frequency selection) para a Europa
- Certificação Wi-Fi Alliance dos seguintes protocolos:
- IEEE 802.11a,b,g,n and ac when it is applicable
- Wi-Fi certified for N
- 2.4 GHz, 5 GHz - Concurrent
- TX 2 tested Spatial Streams 2.4 GHz
- RX 2 tested Spatial Streams 2.4 GHz
- TX 2 tested Spatial Streams 5 GHz

- RX 2 tested Spatial Streams 5 GHz
- Short Guard Interval
- TX A-MPDU
- STBC Transmit
- 40 MHz operation in 2.4 GHz, with coexistence mechanisms
- 40 MHz operation in 5 GHz
- OBSS on Extension Channel
- RIFS Test
- Wi-Fi certified for 11ac when it is applicable
- TX 2 tested Spatial Streams 5 GHz
- Rx 2 tested Spatial Streams 5 GHz
- Rx MCS 8 (256-QAM)
- Rx Short Guard Interval
- TX STBC 2x1
- Rx A-MPDU of A-MSDU
- TX LDPC
- Rx LDPC
- WPA2™ – Enterprise, Personal
- EAP Type(s)
- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC

- EAP-SIM
- EAP-AKA
- EAP-AKA Prime
- EAP-FAST, Personal
- WMM and WMM Power Save

Especificação técnica	Valor
Conectividade	
Interface GE RJ45	1 x 10/100/1000 Base-T
Sistema	
Tipo de Access Point	Indoor
Número de rádios	2 + 1 BT/BLE
Número de antenas	4 internas + 1 interna BT/BLE
Tipo de antenna	Patch: 4 dBi for 2.4 GHz, 5 dBi for 5 GHz
Bandas de frequência (GHz)	2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
Capacidades do Radio 1	2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (256 QAM)
Capacidades do Radio 2	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Taxa máxima de dados	Radio 1: Up to 400 Mbps, Radio 2: Up to 867 Mbps
Bluetooth Low Energy (BT/BLE) Radio	Bluetooth scanning and iBeacon advertisement @ 4 dBm max TX power
Power over Ethernet (PoE)	IEEE 802.3af
SSIDs simultâneos (Máximo)	16

EAP Type(s)	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Autenticação de User/Device	WPA™ and WPA2™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist & whitelist
Potência máxima de transferência	2.4 GHz: 23 dBm / 100 mW 5 GHz: 24 dBm / 251 mW
Especificações IEEE	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3az
Tipos de SSID suportados	Local-Bridge, Tunnel, Mesh
Número de clientes por Radio (Máximo)	512
Coexistência celular	Sim
Modo LED desligado	Sim
Funcionalidade 802.11 avançadas	- 802.11ac Wave 2 MU-MIMO - Transmit Beam Forming (TxBF) - Low-Density Parity Check (LDPC) Encoding - Maximum Likelihood Demodulation (MLD) - Maximum Ratio Combining (MRC) for improved receiver performance - Increased maximum frame transmission by incorporating A-MPDU and A-MSDU Packet Aggregation - Conserve power via Dynamic MIMO power save - Short Guard Interval
Capacidade de Monitorização do Wireless	
Modos de scan de Rogue Radio	Background, Full-time

Modos de radio WIPS / WIDS	Background, Full-time
Modo sniffer de tráfego	Sim
Analisador de espetro	Sim
Energia e Alimentação	
Alimentação AC	SP-FAP200-PA-XX, GPI-115 or GPI-130
Consumo de energia (Máximo)	12.36 W
Temperatura de funcionamento	-20 a 45 °C
Humidade	5 a 90% sem condensação
MTBF (Mean Time Between Failures)	> 30 anos
Certificações	
WiFi Alliance Certified	Sim
DFS	FCC, IC, CE, Japan, Taiwan

3. Solução de distribuição de rede (switch) - FortiSwitch-448E-FPOE

a) O Mecanismo Nacional Anticorrupção pretende adquirir uma solução de distribuição de rede (switch) com funcionalidades de controlo avançado de tráfego, gestão centralizada, suporte a funcionalidades de segurança e fornecimento de energia através de portas PoE+.

b) A solução deve garantir a implementação do ambiente de rede, possibilitar a segmentação da rede e proporcionar alta disponibilidade e desempenho. Adicionalmente, são necessários serviços de suporte técnico especializado premium com uma duração de 3 anos, incluindo implementação, configuração, actualizações de software, manutenção contínua dos equipamentos e assistência técnica, conforme as especificações e requisitos definidos no presente caderno de encargos.

c) Deverá ser comtemplada, formação para 1 pessoa de forma que a mesma fique com os conhecimentos necessários para administração da solução proposta. A referida formação ter de ser dada directamente pelo fabricante ou por um parceiro devidamente habilitado.

d) A unidade deverá possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

Requisitos de Gestão:

As seguintes funcionalidades deverão ser suportadas:

- O equipamento deverá permitir o acesso Telnet / SSH
- O equipamento deverá permitir o acesso HTTP / HTTPS
- O equipamento deverá permitir o acesso via CLI e web GUI interface
- O equipamento deverá permitir configurar SNMP v1/v2c/v3
- O equipamento deverá permitir configurar SNTP
- O equipamento deverá suportar LLDP (802.1ab, Link Layer Discovery Protocol) (receive and transmit)
- O equipamento deverá suportar Loop-guard
- O equipamento deverá suportar POE-pre-standard detection
- O equipamento deverá suportar software download/upload: TFTP/FTP/GUI
- O equipamento deverá suportar Auto Discovery of Multiple Switches
- O equipamento deverá suportar permitir a configuração de VLANs
- O equipamento deverá suportar Syslog Collection
- Deverá ser possível gerir o equipamento através de um Firewall
- O equipamento deverá suportar HTTP REST APIs para configuração e monitorização

Alta Disponibilidade:

As seguintes funcionalidades deverão ser suportadas:

- Multi-Chassis Link Aggregation (MCLAG)

Requisitos de Segurança:

As seguintes funcionalidades deverão ser suportadas:

- O equipamento deverá permitir 802.1x Port Authentication
- O equipamento deverá permitir TACACS+/RADIUS Admin Access
- O equipamento deverá permitir Port Mirroring
- O equipamento deverá permitir Admin Authentication Via RFC 2865 RADIUS
- O equipamento deverá permitir 802.1x authentication with port-based assignment
- O equipamento deverá permitir 802.1x authentication with mac-based assignment
- O equipamento deverá permitir sFlow
- O equipamento deverá permitir ACL Tables
- O equipamento deverá permitir QOS: 802.1p support
- O equipamento deverá permitir VLAN tag by ACL
- O equipamento deverá permitir VLAN tag by MAC/IP/802.1x

Requisitos de Routing:

As seguintes funcionalidades deverão ser suportadas:
O equipamento deverá permitir Inter-VLAN Routing

- O equipamento deverá permitir Static Routing (Software-based only) routing (like management traffic)

- O equipamento deverá permitir Static Routing (Hardware-based)
- O equipamento deverá permitir L3 Host/ARP Entries
- O equipamento deverá permitir Static BFD (Bidirectional Forwarding Detection)

Requisitos de Layer 2

As seguintes funcionalidades deverão ser suportadas:

- O equipamento deverá suportar Jumbo Frames
- O equipamento deverá suportar auto negociação da velocidade dos portos e duplex
- O equipamento deverá suportar IEEE 802.1D MAC Bridging/STP
- O equipamento deverá suportar EEE 802.1w Rapid Spanning Tree Protocol
- O equipamento deverá suportar EEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- O equipamento deverá suportar Edge Port / Port Fast
- O equipamento deverá suportar EEE 802.1Q VLAN Tagging
- O equipamento deverá suportar EEE 802.3ad Link Aggregation com LACP
- O equipamento deverá suportar balanceamento de tráfego Unicast/Multicast sobre portos em trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- O equipamento deverá suportar EEE 802.1AX Link Aggregation
- O equipamento deverá suportar Spanning Tree Instances (MSTP/CST)
- O equipamento deverá suportar IEEE 802.3x Flow Control and back-pressure
- O equipamento deverá suportar IEEE 802.3 10Base-T
- O equipamento deverá suportar IEEE 802.3u 100Base-TX
- O equipamento deverá suportar IEEE 802.3z 1000Base-SX/LX
- O equipamento deverá suportar IEEE 802.3ab 1000Base-T

- O equipamento deverá suportar 802.3 CSMA/CD Access Method and Physical Layer Specifications
- O equipamento deverá suportar MAC, IP, Ethertype-based VLANs
- O equipamento deverá suportar Virtual-Wire

Requisitos de Serviços:

As seguintes funcionalidades deverão ser suportadas:

- O equipamento deverá suportar IGMP Snooping (v1/v2/v3)
- O equipamento deverá suportar IP conflict detection & notification

Requisitos ao nível do suporte de RFC e MIB:

As seguintes funcionalidades deverão ser suportadas:

- RFC 2571 Architecture for Describing SNMP Framework
- DHCP relay feature
- DHCP Snooping
- RFC 854 Telnet Server
- RFC 2865 RADIUS
- RFC 1643 Ethernet-like Interface MIB
- RFC 1213 MIB-II
- RFC 1354 IP Forwarding Table MIB
- RFC 2572 SNMP Message Processing and Dispatching
- RFC 1573 SNMP MIB II
- RFC 1157 SNMPv1/v2c
- RFC 2030 SNTP

Especificação técnica	Valor
Conectividade	
Nº total de interfaces	48x GE RJ45 4x 10GE SFP+ ports
Nº de portas PoE	48
Capacidade de PoE	772 W
Interface de gestão dedicada 10/100 Mbps	1
Interface Consola RJ45	1
Sistema	
Modo de gestão	Web e por CLI
Capacidade de switching (Duplex)	176 Gbps
Pacotes por segundo (Duplex)	262 Mpps
Armazenamento de MAC addresses	32 000
Latência	< 1µs
Número de VLANs suportadas	4000
IPv4/IPv6 Dual Stack Routing Ready Hardware	Sim
Tamanho do grupo Link Aggregation Group	até 8
Número total de Link Aggregation Groups	52
Capacidade da DRAM	1 GB
Capacidade da FLASH	256 MBs
Funcionalidades L3	Incluídas
Stackable	SIM
MTBF (Mean Time Between Failures)	>10 anos
Energia e Alimentação	
Alimentação AC	100–240V AC, 50–60 Hz

Consumo de energia máximo	até 923.6W
Dissipação Térmica	163.1 BTU/h
Fonte de alimentação redundante	SIM
Condições ambientais	
Temperatura de funcionamento	0 - 50 °C
Humidade	10 to 90% sem condensação

4. Solução de Alimentação Ininterrupta (UPS) - APC Smart-UPS 1000VA LCD RM 2U

O Mecanismo Nacional Anticorrupção pretende adquirir uma solução de alimentação ininterrupta (UPS) que garanta a protecção dos equipamentos de rede e sistemas críticos contra falhas de energia, assegurando continuidade de serviço e alta disponibilidade.

A unidade deverá possuir um conjunto de especificações e tecnologias, conforme detalhado a seguir:

- Capacidade de saída: Mínimo de 1000VA / 700W para suportar a carga de firewalls, switches e outros equipamentos de rede críticos.
- Tensão de entrada/saída nominal: 230V com suporte a variações de tensão, ajustável para 208V, 220V, 230V ou 240V.
- Tempo de autonomia a plena carga: Mínimo de 6 minutos a 700W.
- Tempo de autonomia a meia carga: Mínimo de 18 minutos a 350W.
- Capacidade de expansão de baterias: Suporte para baterias externas para aumentar a autonomia, se necessário.
- Tempo de recarga: Tempo de recarga de bateria completa em até 3 horas.
- Formato rackmount: Unidade com montagem em rack de 2U para integração em bastidores de 48U ou padrão equivalente.
- Porta USB: Para monitorização local e integração com software de gestão.
- Porta série: Suporte para comunicação com sistemas mais antigos.

- Slot de expansão (SmartSlot): Para instalação de placas de rede e gestão remota via SNMP.
- Suporte a APC PowerChute ou equivalente, para shutdown automático e gestão centralizada.
- Topologia: Line Interactive com regulação automática de tensão (AVR) para protecção contra flutuações de energia sem recorrer à bateria.
- Forma de onda de saída: Onda senoidal pura, garantindo alimentação de alta qualidade para equipamentos sensíveis.
- Protecção contra picos de tensão: Capacidade de supressão de picos de até 459 joules.
- Eficiência a plena carga: Mínimo de 97% em modo económico (Green Mode) para reduzir o consumo energético.
- Faixa de temperatura: Operação garantida entre 0°C e 40°C.
- Humidade relativa: Operação entre 0% e 95% sem condensação.
- Certificações: Deve cumprir com os padrões CE, TUV, EN/IEC 62040-1, EN/IEC 62040-2, ou equivalentes.

5. Solução de Bastidor Rack para instalação do equipamento de rede

O Mecanismo Nacional Anticorrupção pretende adquirir um bastidor de 18U para alojamento e organização de equipamentos de rede, servidores, dispositivos de armazenamento e sistemas de alimentação ininterrupta (UPS).

O bastidor deve assegurar gestão eficiente de cabos, ventilação adequada, segurança física, possuir pelo menos um bloco PDU e deve ser compatível com equipamentos padrão de 19 polegadas.

Dimensões e Capacidade

Altura: 18U.

Largura: 600 mm (padrão 19 polegadas, compatível com EIA-310).

Profundidade: 1070 mm.

Estrutura e Construção

Material: Construção em aço laminado a frio, com elevada durabilidade.

Porta frontal: Porta em malha perfurada com ventilação de 80%, com fechadura de segurança e acesso reversível.

Portas traseiras: Porta dupla perfurada para facilitar o fluxo de ar e o acesso aos equipamentos.

Painéis laterais: Removíveis, com fecho rápido, permitindo fácil acesso durante a instalação e manutenção.

Gestão de Cabos

Passagens de cabos superiores e inferiores: Com tampas de escova para permitir a entrada e saída de cabos sem comprometer a organização.

Gestão vertical de cabos: Inclui organizadores laterais para arrumar os cabos de forma eficiente e proteger contra dobras ou emaranhados.

Ventilação e Refrigeração

Ventilação natural: Portas frontal e traseira perfuradas, optimizando o fluxo de ar natural e melhorando a refrigeração passiva dos equipamentos.

Compatível com sistemas adicionais de ventilação: Suporte para instalação de ventiladores ou unidades de ar condicionado dedicadas.

Gestão de Energia

PDUs: Deverá possuir, no mínimo, uma Unidade de Distribuição de Energia (PDU) com, pelo menos, oito tomadas no interior do bastidor.

Aterramento: Sistema integrado de aterramento para garantir a protecção eléctrica dos dispositivos.

Segurança Física

Fechaduras de segurança: Porta frontal e traseira com fechadura de chave única, para prevenir acesso não autorizado aos equipamentos.

Preparado para sensores ambientais: Compatível com sensores para monitorização de ambiente, como temperatura, humidade e portas abertas, para aumentar a segurança física e electrónica.

Compatibilidade

Padrão EIA-310: Totalmente compatível com equipamentos de 19 polegadas (servidores, switches, UPSs, etc.).

Trilhos ajustáveis: Trilhos de montagem ajustáveis, permitindo a instalação de equipamentos com diferentes profundidades.

6. **Aquisição de Licenças Windows 11**

O **Mecanismo Nacional Anticorrupção** pretende adquirir **30 licenças do Windows 11 Enterprise** com o objectivo de substituir as licenças actualmente em uso, fornecidas pelo **IGFEJ**, assegurando a continuidade operacional e a modernização tecnológica.

Tipo de Licença

- **Produto**: Microsoft Windows 11 Enterprise.
- **Tipo de Licenciamento**: Licença perpétua.
- **Modalidade de Licenciamento**:
  - Open License, CSP (Cloud Solution Provider), ou qualquer modalidade apropriada, compatível com a possível integração numa solução Cloud existente ou futura.
- **Licenciamento por Dispositivo ou por Utilizador**: A determinar, conforme o modelo que melhor se adeque às necessidades institucionais.

Versão e Idioma

- **Versão**:

- Windows 11 Enterprise (última versão estável disponível à data da aquisição, com suporte para actualizações regulares de segurança e funcionalidades).

- **Idioma**:
  - Multilíngue, com suporte completo para Português Europeu.

Compatibilidade e Requisitos

- **Compatibilidade com Infra-estruturas Existentes**:
  - Integração nativa com **Microsoft Active Directory** e **Azure Active Directory**.
  - Suporte para gestão centralizada através do **Microsoft Endpoint Manager (Intune)**.
- **Requisitos Mínimos de Hardware**:
  - Compatível com dispositivos existentes, incluindo suporte para:
    - Processador compatível com arquitectura x86/x64 de 64 bits.
    - Trusted Platform Module (TPM) 2.0 ativado.
    - Configuração de hardware conforme os requisitos do Windows 11 Enterprise (CPU, RAM, armazenamento e gráficos).

Funcionalidades Específicas

- **Gestão Centralizada de TI**:
  - Suporte avançado para políticas de segurança e gestão de dispositivos.
- **Segurança Avançada**:
  - BitLocker, Credential Guard, e Windows Defender Application Control.
- **Colaboração e Produtividade**:
  - Integração optimizada com Microsoft Teams e ferramentas da suíte Microsoft 365.

- **Virtualização**:
  - Total compatibilidade com tecnologias como Hyper-V e ambientes VDI (Virtual Desktop Infrastructure).

Garantia e Suporte

- **Conformidade**:
  - Garantia de conformidade integral com as políticas e regulamentações de licenciamento da Microsoft.
- **Actualizações e Manutenção**:
  - Garantia de acesso a actualizações de segurança e funcionalidades enquanto o produto estiver em suporte pela Microsoft.

7. Solução de serviços Cloud - Microsoft Azure

O Mecanismo Nacional Anticorrupção (MENAC) tem como objectivo a contratação de serviços de cloud computing que proporcionem uma infra-estrutura flexível e escalável, de modo a sustentar as suas operações digitais.

A solução contratada será válida por um período de 12 meses e deverá englobar serviços de computação, armazenamento, gestão de bases de dados, redes, segurança, gestão de identidades, backups, recuperação de desastres e monitorização contínua, assegurando, simultaneamente, elevada disponibilidade, desempenho optimizado e protecção de dados. Além disso, o serviço Cloud deverá disponibilizar 30 licenças de aplicações de produtividade e colaboração.

Adicionalmente, requer-se suporte técnico especializado que garanta a correcta implementação, configuração, optimização e manutenção da plataforma, em conformidade com as especificações técnicas e os requisitos estabelecidos no presente caderno de encargos.

Requisitos Técnicos Solução Cloud:

- Cloud Firewall

- Cloud DNS
- Cloud Entra ID (Cloud AD)
- Cloud Virtual Desktop
- Cloud Backup
- Content Delivery Network
- App Service
- Cloud Database for MySQL
- Largura de Banda (Bandwidth)
- Endereços IP (IP Addresses)
- Recognize
- OpenAI
- Embeddings
- Document intelligence

Para assegurar uma gestão centralizada, a plataforma Cloud deverá disponibilizar um portal self-service. O custo de computação deve basear-se na utilização real, permitindo, através da consola, ajustar imediatamente e a qualquer momento os recursos alocados. A solução deve evitar custos de computação quando os servidores estão desligados e possibilitar a orquestração automática para ligar e desligar servidores.

Funcionalidades Adicionais:

- Plataforma de Backups incluída, com uma cópia secundária a mais de 300 km de distância, dentro da União Europeia.
- Plataforma de Antimalware para todos os servidores da solução.
- SLA (nível de serviço) mínimo de 99,9% para os serviços de infra-estrutura.
- Possibilidade de activação de georrelicação de dados entre dois datacenters na União Europeia, de forma automática.

Segurança:

- A solução de cloud pública deverá possuir certificação nas normas ISO/IEC 27001, garantindo a segurança da informação e protecção contra ameaças.
- A solução de cloud pública deverá também possuir certificação na norma ISO/IEC 27018, assegurando a protecção de dados pessoais em conformidade com a legislação europeia sobre privacidade.
- Detalhe de logs e eventos dos serviços aprovisionados pelo cliente.
- Encriptação de dados em repouso e em trânsito entre datacenters.
- Controlo total sobre o acesso do Cloud Provider aos dados da MENAC.
- Mecanismos de segurança proactivos, com recomendações de melhorias específicas por serviço.
- A infra-estrutura de cloud pública deverá ainda possuir no mínimo 3 anos consecutivos de certificação de segurança de grau Nacional Reservado do Gabinete Nacional de Segurança (GNS), garantindo que os dados sensíveis da MENAC estão devidamente protegidos e auditados conforme as normas de segurança nacionais.

Privacidade e Controlo:

- Serviços de encriptação com chaves próprias.
- Escolha da localização de armazenamento dos dados em repouso, com possibilidade de os manter em pelo menos duas localizações na União Europeia.
- Garantia de remoção total dos dados da MENAC a pedido e após o término do contrato.
- Proibição de utilização dos dados da MENAC, ou informações derivadas, para publicidade ou fins comerciais semelhantes.

Conformidade e Transparência:

- Disponibilização de relatórios de auditoria efectuados por entidades terceiras.
- Acesso à informação sobre o cumprimento de standards relevantes por cada serviço Cloud prestado.
- Relatórios de auditoria por entidades independentes.
- Informação online sobre o estado dos diferentes serviços Cloud (disponibilidade e desempenho) e histórico de incidentes, com um mínimo de um mês.
- Comunicação proactiva de falhas de serviço por parte do prestador de serviços Cloud.

Estimativa de Utilização Anual de Tokens

Para o correto planeamento orçamental e técnico relacionado com o uso de serviços **Azure OpenAI**, o **Mecanismo Nacional Anticorrupção (MENAC)** estima a seguinte utilização anual de tokens:

1. Azure OpenAI - GPT-4 (modelo gpt-4o-2024-08-06)

- **Tokens estimados anualmente**:
  - **3 802 933 000 tokens/ano** para operações principais (caso de uso primário).
  - **564 000 000 tokens/ano** para operações adicionais (caso de uso secundário).
- **Total estimado**: 4 366 933 000 tokens/ano.

2. Embeddings Azure - Modelo text-embedding-ada-002

- **Tokens estimados anualmente**:
  - **1 901 466 667 tokens/ano** para geração de embeddings (caso de uso principal).

Resumo Global de Consumo Estimado

Serviço	Modelo	Tokens/ano
Azure OpenAI	gpt-4o-2024-08-06 (primário)	3 802 933 000
Azure OpenAI	gpt-4o-2024-08-06 (secundário)	564 000 000
Azure Embeddings	text-embedding-ada-002	1 901 466 667
Total (todos os serviços)		**6 268 399 667**

Notas Adicionais

a) **Orçamento Baseado em Tokens**:

   a. Recomenda-se que os custos de licenciamento e utilização sejam calculados com base nas taxas unitárias por 1 000 tokens fornecidas pela **Azure OpenAI Service** e outros fornecedores relevantes.

b) **Dimensão e Escalabilidade**:

   a. Estes valores são uma projeção anual e podem variar conforme o crescimento das necessidades do MENAC. É importante prever flexibilidade para escalabilidade adicional.

8. Aplicação de Produtividade Microsoft Office 365 E5 EEA

Aplicações de Escritório e Colaboração Empresarial O serviço Cloud deverá disponibilizar 30 licenças de aplicações de produtividade e colaboração empresarial, com as seguintes funcionalidades:

- Aplicações de Escritório:

  ➢ Acesso a ferramentas completas de produtividade, incluindo processador de texto, folha de cálculo, apresentações, e-mail corporativo com armazenamento generoso, e aplicações de notas e bases de dados.

- Armazenamento pessoal na cloud com capacidades de partilha e colaboração em tempo real.
- Ferramentas avançadas de análise de dados e criação de relatórios.
- Funcionalidades de segurança, encriptação de dados e conformidade com regulamentos de proteção de dados.
- A aplicação de produtividade deverá possuir certificação de segurança de grau Nacional Reservado do Gabinete Nacional de Segurança (GNS).

9. **Plataforma de Colaboração Empresarial Microsoft Teams EEA**:

- Funcionalidades de chat, videochamadas e reuniões online para colaboração em tempo real.
- Suporte para reuniões de grande escala com centenas de participantes e eventos online com até 10.000 pessoas.
- Integração com outras aplicações e ferramentas de produtividade.
- Gravação de reuniões, transcrições automáticas e gestão de eventos online.
- Ferramentas de segurança e conformidade, como encriptação de dados em trânsito e repouso, controlo de acessos e gestão de dados.
- Análises de utilização para otimização da produtividade e colaboração.

10. Requisitos Técnicos do Fornecedor de Serviços

A empresa concorrente deverá demonstrar competências comprovadas para a prestação de serviços técnicos especializados no âmbito das tecnologias Microsoft, apresentando certificações ou reconhecimentos que atestem as suas capacidades técnicas, de acordo com os seguintes critérios:

a. Requisitos Obrigatórios

Os seguintes itens de certificação técnica são considerados indispensáveis para garantir a capacidade técnica do fornecedor na execução do contrato:

i. **Licenciamento e Gestão de Ativos**:

- Microsoft Certified Volume Licensing Specialist, Large Organizations.
- Microsoft Certified Designing, Assessing and Optimizing Software Asset Management (SAM).

ii. **Gestão de Infraestrutura e Cloud**:

- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified: Windows Server Hybrid Administrator Associate.

9.1.3. Segurança e Compliance:

- Microsoft 365 Certified: Security Administrator Associate.
- Microsoft Certified: Security, Compliance, and Identity Fundamentals.

9.1.4. Gestão e Suporte:

- Trainer: MCT Enrollment (competências pedagógicas).

Nota: O cumprimento de 100% dos itens obrigatórios é exigido para a qualificação técnica no procedimento.

2. Requisitos Preferenciais

Os seguintes itens de certificação técnica serão considerados como elementos diferenciadores, valorizando a proposta do concorrente:

1. **Microsoft 365**:
    - Microsoft 365 Certified: Administrator Expert.
    - Microsoft 365 Certified: Messaging Administrator Associate.
    - Microsoft Certified Solutions Associate: Office 365.
2. **Segurança Avançada**:
    - Microsoft Certified: Security Operations Analyst Associate.
    - Microsoft Certified Solutions Expert: Productivity.
3. **Cloud e Virtualização**:

- Microsoft Certified: Azure AI Fundamentals.
- Microsoft Certified: Azure Virtual Desktop Specialty.

4. **Reconhecimentos**:
   - Microsoft MVP (Most Valuable Professional): M365 Apps & Services.

Nota: Cada item preferencial cumprido será pontuado conforme os critérios de análise definidos.

3. Equivalência de Certificações

Serão aceites certificações ou comprovativos equivalentes que demonstrem competências idênticas às exigidas, mediante avaliação pela entidade adjudicante.