



CONTRATO Nº 35/2022 AQUISIÇÃO DE EQUIPAMENTO E INFORMÁTICO – LOTE 10 PELA ESCOLA SUPERIOR DE ENFERMAGEM DE COIMBRA, AO ADJUDICATÁRIO NS IT, LDA., PELA QUANTIA TOTAL DE 71 955,24€ (SETENTA E UM MIL NOVECENTOS E CINQUENTA E CINCO EUROS E VINTE E QUATRO CÊNTIMOS), ACRESCIDO DE IVA

Aos vinte e oito dias do mês de dezembro de 2022, na Escola Superior de Enfermagem de Coimbra, sita na Rua 5 de Outubro– 3045 -043 Coimbra, compareceram: -----

A Escola Superior de Enfermagem de Coimbra, com o contribuinte nº 600081583, adiante designada por **ESEnfC**, representada pelo Professor Doutor António Fernando Salgueiro Amaral, Presidente, por eleição homologada pela Ministra da Ciência, Tecnologia e Ensino Superior, publicada por Despacho nº 10534/2022, de 30 de agosto, que outorga em nome da ESEnfC, da qual é representante legal, como primeiro outorgante, e-----

NS IT, Lda., pessoa coletiva nº 515915017, com sede na Rua de Santana, 963, C- Sala 14, 4465-742 Leça do Balio, representada por Hélder Miguel Ferreira Henriques, titular do cartão do cidadão n.º

na qualidade de sócio gerente, pessoa cuja identidade e poderes para o ato foram legalmente reconhecidos e que pode outorgar, conforme documentação apresentada e que se anexa ao processo, como segunda outorgante.-----

Pelo primeiro outorgante foi dito que após ter sido autorizada a abertura de procedimento decorrente do presente contrato por despachos do Presidente de 29-09-2022 e aprovada a adjudicação e respetiva minuta em 21-12-2022, após a realização do Procedimento de Concurso Público com a referência Concurso Público nº 16/2022, ao abrigo do art.º 20º nº1 b) do CCP, com o nº de compromisso 2022/551, o presente contrato vai reger-se de acordo com as cláusulas seguintes:-----



PARTE I - Cláusulas jurídicas

Artigo 1º | Objeto

O presente contrato é celebrado na sequência do procedimento pré-contratual ao abrigo do art.º 20º nº1 c) Código dos Contratos Públicos (CCP), na atual redação, e que tem por objeto a aquisição de equipamento informático, Lote 10.-----

- Projeto designado por Residência da ESENFcoimbra - MF_28_RE/2022/PRR/PNAES, Contrato-Programa de Financiamento N.º 10_01/CO2-i06/2022, no âmbito do Programa Nacional de Alojamento para o Ensino Superior (PNAES), apoiado pelo Plano de Recuperação e Resiliência (PRR) – Lote 10. ----

O fornecimento com o código CPV 30237110-3 conforme legislação em vigor. -----

Artigo 2º | Local da entrega dos equipamentos

Os bens objeto deste procedimento serão entregues no edifício da ESEnFC, sito Rua 5 de Outubro – S. Martinho do Bispo – Coimbra – Serviço de Aprovisionamento ou noutra edifício da Escola. -----

Artigo 3º | Prazo

1. O início para o fornecimento será após a data da notificação do relatório final de adjudicação, devendo estar integralmente concluído em 30 dias. -----
2. Caso os objetos adjudicados não se encontrem entregues dentro do prazo, **implicará o incumprimento do contrato** relativamente aos produtos não entregues.-----

Artigo 4º | Contrato e Prevalência

1. O contrato é reduzido a escrito de acordo com nº 1 do art. 94º e o art.º. 95º do CCP e é composto pelo respetivo clausulado contratual e os seus anexos. -----
2. Fazem ainda parte integrante do contrato documentos conforme nº 2 do art.96º do CCP:-----
3. Além dos documentos indicados nos números anteriores, a entidade fornecedora obriga-se também, a respeitar, no que lhe seja aplicável e não esteja em oposição com os documentos do contrato, as normas portuguesas e europeias, as especificações e documentos de homologação de organismos oficiais, e as de fabricantes ou de entidades detentoras de patentes. -----



4. Em caso de divergência entre os documentos referidos no nº 2, a respetiva prevalência é determinada pela ordem pela qual aí são indicados. -----
5. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do CCP e aceites pelo adjudicatário, nos termos do disposto no artigo 101.º desse mesmo diploma legal. -----

Artigo 5º | Condições de pagamento

1. O preço será pago, por adjudicação e por cada lote, devendo a respetiva liquidação ser feita até ao limite de 30 (trinta) dias, da apresentação da fatura e de acordo com a Nota de Encomenda emitida pela adjudicante, sendo o seu pagamento efetuado por transferência bancária, contra a apresentação de recibo. -----
2. Nas faturas deve ser indicado o número de compromisso que consta na Nota de Encomenda. -----
3. Nas condições de pagamento não podem ser propostos adiantamentos por conta do fornecimento a efetuar. -----
4. Ao abrigo do nº1 do art. 299º-B do CCP as faturas deverão ser eletrónicas, através de Intercâmbio Eletrónico de Dados, disponibilizado pela YET - Your Electronic Transactions, Lda. (YET) (intervan@yetspace.com), assim deve ser estabelecido contacto com a (YET) (sales@yetspace.com, telefone 253149253). -----
5. Poderão ser realizados adiantamentos de preço por conta de prestações/fornecimentos a realizar ou de atos preparatórios ou acessórios das mesmas se cumprido o disposto no art. 292º do CCP. Em casos excecionais, podem ser efetuados adiantamentos sem que estejam reunidas as condições previstas nos números 1 e 2 do art. 292º do CCP, de acordo com o legalmente previsto.

Artigo 6º | Sigilo e proteção de dados

1. O cocontratante garantirá sigilo e confidencialidade sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à ESEnFC, de que os seus funcionários venham a ter conhecimento no âmbito da sua execução, sendo extensível aos seus agentes, funcionários, colaboradores ou terceiros ao abrigo ou em relação com a execução do contrato. -----



2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato. -----
3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo prestador de serviços 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. -----
4. A quebra de sigilo profissional imputável a pessoal adstrito ao adjudicatário, poderá constituir à entidade adjudicante o direito à denúncia unilateral do contrato de adjudicação. -----
5. A entidade adjudicatária na execução dos serviços e os seus trabalhadores ou colaboradores, independentemente do seu vínculo contratual, declara que cumpre a aplicação do Regulamento Geral sobre a Proteção de dados (Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e demais, legislação em vigor. -----

Artigo 7º | Cessão da posição contratual

1. O cocontratante não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da contratante pública. -----
2. Para efeitos da autorização prevista no número anterior, e nos termos do art 318º do CCP, deve apresentar toda a documentação de habilitação exigida ao adjudicatário no presente procedimento. -----

Artigo 8º | Incumprimento por facto imputável ao cocontratante e resolução sancionatória

1. Se o cocontratante não cumprir de forma exata e pontual as obrigações contratuais ou parte delas por facto que lhe seja imputável, deve o contraente público notificá-lo para cumprir dentro de um prazo razoável, salvo quando o cumprimento se tenha tornado impossível ou o contraente público tenha perdido o interesse na prestação. -----
2. Mantendo -se a situação de incumprimento após o decurso do prazo referido no número anterior, o contraente público pode optar pela efetivação das prestações de natureza fungível em falta,



- diretamente ou por intermédio de terceiro, ou por resolver o contrato com fundamento em incumprimento definitivo, nos termos do disposto no artigo 333.º do CCP. -----
3. Para efeitos do disposto no número anterior, considera-se incumprimento definitivo quando houver atraso na prestação dos serviços/fornecimento ou falta de reposição de bom funcionamento por período superior a 10 dias úteis.-----
 4. Se o contraente público optar pela execução das prestações fungíveis por terceiro, à formação do contrato com esse terceiro é aplicável o disposto na Parte II do CCP.-----
 5. O disposto nos números anteriores não prejudica a aplicação pelo contraente público de sanções previstas no contrato ou lei, se previstas, para o caso de incumprimento pelo cocontratante, por facto que lhe seja imputável, nem a aplicação das disposições relativas à obrigação de indemnização por mora e incumprimento definitivo previstas no Código Civil, sendo o montante deduzido das quantias devidas nos termos do nº 3 do art. 333º do CCP. -----
 6. A resolução do contrato com base nos pontos anteriores determinará a execução total ou parcial do direito à caução prestada, se aplicável, e não dará lugar a qualquer indemnização por parte do contratante.-----
 7. O disposto na cláusula anterior não prejudica o pagamento dos serviços já efetuados em conformidade com as cláusulas contratuais.-----
 8. O direito de resolução referido exerce-se mediante declaração enviada ao cocontratante.-----

Artigo 9º | Casos fortuitos ou de força maior

1. Não podem ser impostas penalidades ao cocontratante, 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, designadamente greves ou outros conflitos coletivos de trabalho, 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. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação. -----



Artigo 10° | Patentes, licenças e marcas registadas

1. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças. -----
2. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o adjudicatário indemniza-o de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for. -----

Artigo 11° | Fiscalização do modo de execução do contrato

O contraente público dispõe de poderes de fiscalização conforme o estipulado no art. 305º do CCP. --

Artigo 12° | Foro competente

Para todas as questões emergentes do presente contrato será competente o Tribunal Administrativo e Fiscal de Coimbra ou o Tribunal da Comarca de Coimbra. -----

Artigo 13° | Comunicações e notificações

Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes contratuais, estas devem ser escritas e redigidas em português, nos termos previstos no CCP art.468º e segs, e dirigidas para o domicílio ou sede contratual de cada uma, identificados no contrato e qualquer alteração das informações de contacto constantes do documento outorgado deve ser comunicada à outra parte. -----

Artigo 14° | Contagem dos prazos

Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados salvo quando expressamente previstos dias úteis. -----



Artigo 15º | Legislação aplicável

O contrato é regulado pela legislação portuguesa. -----

PARTE II - Cláusulas técnicas

Artigo 16º | Obrigações do contratante público

São obrigações do contratante: -----

1. Fornecer ao cocontratante todas informações sobre o local de entrega dos bens, e combinar a data de entrega do mesmo dentro do prazo estabelecido.-----
2. No ato do fornecimento dos bens, procederá à verificação quantitativa e qualitativa dos mesmos.
3. A rejeição dos bens por parte da entidade adjudicante pode conferir-lhe o direito a ser indemnizada pelos custos incorridos e pelos danos sofridos. -----
4. Suspender a faturação e correspondente pagamento até que a situação se encontre regularizada relativamente a fornecimento de bens em quantidades inferiores às encomendadas ou com qualidade insuficiente.-----

Artigo 17º | Obrigações do cocontratante

São obrigações do cocontratante:

1. Fornecer os bens descritos conforme caderno de encargos e constante no mapa de quantidades anexo.-----
2. Realizar a entrega dos bens em qualquer dos Polos da Escola Superior de Enfermagem de Coimbra.
3. Os encargos e organização da entrega dos bens nas instalações da entidade adjudicante são da responsabilidade do contratante.-----
4. O cocontratante obriga-se a cumprir o prazo de entrega, a contar da data da notificação do relatório final de adjudicação, **no prazo de 30 dias.** -----
5. No caso de a entidade fornecedora não possuir para entrega, nos prazos definidos, os bens encomendados, deverá propor a sua substituição por outros de qualidade idêntica ou superior, não



- podendo, deste facto, resultar acréscimo de preço dos respetivos bens. A entidade fornecedora dispõe de um prazo de 2 dias úteis a contar da comunicação para suprir as deficiências e irregularidades detetadas durante a instalação, que não impliquem a rejeição dos equipamentos. -----
6. Na situação prevista no número anterior, a entidade fornecedora deverá fornecer todos os elementos necessários à avaliação da adequação da substituição por parte da entidade pública, nomeadamente amostras, fotografias e especificações técnicas dos bens. Contudo, em caso algum fica a adjudicante obrigada a aceitar a substituição dos bens propostos pelo fornecedor. -----
 7. No caso de rejeição dos bens por deficiências de qualidade *o adjudicatário fica obrigado à sua imediata substituição*, continuando para efeitos de aplicação de sanções, a correr a contagem do prazo de entrega, desde a data da encomenda até à finalização do fornecimento de acordo com as exigências estabelecidas, não conferindo a rejeição dos bens qualquer direito a qualquer indemnização. -----
 8. Todos os encargos decorrentes da substituição, devolução ou destruição dos bens que tenham sido objeto de rejeição, serão da exclusiva responsabilidade do fornecedor.-----
 9. O fornecimento de bens em quantidades inferiores às encomendadas ou com qualidade insuficiente, suspenderá a faturação e correspondente pagamento até que a situação se encontre regularizada.-----
 10. O adjudicatário obriga-se a apresentar à entidade adquirente, sempre que esta lhe solicite, todos os documentos e informações relativos ao fornecimento, designadamente: -----
 11. Documentos comprovativos da titularidade das autorizações, certificados ou licenças legalmente exigidas para o fornecimento contratado, cumprindo as normas portuguesas e europeias, as especificações e documentos de homologação de organismos oficiais, e as de fabricantes ou de entidades detentoras de patentes. -----
 12. Não transferir ou ceder a terceiros, sem o consentimento escrito do contratante público, os direitos e obrigações emergentes do contrato que vier a ser celebrado na base deste caderno de encargos. -----
 13. Garantir o cumprimento das Diretiva 2011/65/UE (RoHS), de 8 de junho, transporta para a ordem jurídica interna pelo Decreto-Lei nº 79/2013, de 11 de junho, da Diretiva nº 2012/19/UE (REEE),



- de 4 de julho, e da Diretiva e 2006/66/CE, de 6 de setembro, transpostos para a ordem jurídica interna pelo n.º 6/2009 de 6 de janeiro. -----
14. Garantir o cumprimento do Decreto-lei n.º 209/1999, respeitante à classificação, embalagem e rotulagem das substâncias perigosas. -----
15. Os produtos, a fornecer com os cabos necessários ao seu funcionamento, serão instalados nos locais definidos pela entidade adquirente e/ou contratante. -----
16. As embalagens dos produtos devem ser conservadas fechadas e seladas pela entidade fornecedora até à instalação dos mesmos, se aplicável. -----
17. Os riscos nas fases de transporte, acondicionamento, embalagem, carga e descarga da entrega, são da exclusiva responsabilidade da entidade fornecedora e/ou prestadora de serviços. -----
18. A entidade fornecedora e/ou prestadora de serviços será responsável pela instalação dos equipamentos em condições normais de funcionamento, devendo, nomeadamente: -----
- a. garantir o funcionamento de todas as funcionalidades, incluindo a instalação do sistema operativo nos casos aplicáveis, solicitadas pela entidade adquirente e/ou contratante; -----
 - b. disponibilizar uma ficha técnica para registos relativos à assistência técnica; -----
 - c. disponibilizar para cada equipamento um manual de utilizador e um manual de referência rápida, em Português; e -----
 - d. disponibilizar o manual de utilizador referido anteriormente em formato eletrónico. -----
19. A entidade fornecedora dispõe de um **prazo máximo de 10 dias úteis** a contar da comunicação para proceder à substituição dos equipamentos em caso de rejeição dos mesmos. -----
20. A rejeição dos produtos disponibilizados nos termos do presente artigo não confere à entidade fornecedora e/ou prestadora de serviços o direito a qualquer indemnização, contudo a rejeição dos produtos por parte da entidade adquirente e/ou contratante pode conferir-lhe o direito a ser indemnizada, pelos custos incorridos e prejuízos comprovadamente sofridos. -----

Artigo 18º | Equipamentos a fornecer e a instalar

1. -- Os equipamentos deverão apresentar uma **garantia mínima de 3 anos**, exceto quando não aplicável, e de acordo com a proposta apresentada. -----



2. -- Todos os equipamentos devem cumprir integralmente todas as especificações técnicas do anexo A que faz parte integrante do Caderno de Encargos.-----

3. -- Bens a fornecer:-----

Lote 10 – Equipamento de acesso Wireless -----

10.1 – Equipamento – 2 unidades -----

a) A nível de Segurança de rede:-----
firewalls do fabricante Fortinet, modelo FG-401F, ou equivalente, cumprindo os requisitos (2 unidades):-----

Pretende-se que a componente de segurança da solução seja suportada por 2 equipamentos de firewall que apresentem as seguintes características técnicas:-----

Conectividade-----

- 16 Interfaces GE RJ45 Aceleradas por Hardware-----
- 8 Interfaces 1GE SFP Aceleradas por Hardware-----
- 4 Interfaces 1GE / 10GE SFP+ Aceleradas por Hardware-----
- 4 Interfaces 10GE SFP+ Ultra Low Latency Aceleradas por Hardware-----
- 1 Interface de Gestão GE RJ45-----
- 1 Interface de HA GE RJ45-----
- 1 Interface USB-----
- 1 Interface de Console (RJ45)-----

Sistema-----

- 2 Discos internos de 480GB SSD cada-----
- Trusted Platform Module (TPM)-----

Desempenho-----

- Aceleração do tráfego de Firewall e IPSec por hardware dedicado-----



- Aceleração de tráfego NGFW por hardware dedicado-----
- Políticas de firewall, no mínimo 9 000 -----
- Túneis IPSec cliente remoto, no mínimo 45 000-----
- VPN SSL - Máximo de utilizadores simultâneos, no mínimo 4500-----
- Access points controlados centralmente, no mínimo 500 -----
- Domínios virtuais, no mínimo 8-----
- Licenciamento ilimitado de utilizadores -----

Energia e Alimentação-----

- Alimentação AC 100-240V AC, 50-60Hz-----
- Consumo de energia máximo 198 W -----
- Fontes de alimentação redundantes (hot swappable) -----

Condições ambientais-----

- Temperatura de funcionamento entre os 0 e os 40° C-----
- Humidade entre os 5% e os 90% sem condensação -----
- Fluxo de ar de frente e lados para trás-----

Integração com redes de comunicações-----

As seguintes funcionalidades deverão ser suportadas: -----

- Servidor de DHCP, NTP e DNS incluído-----
- Funcionalidade de DNS Proxy -----
- Múltiplos modos de configuração de interfaces:-----
 - Sniffer-----
 - Agregação de portas (802.3ad)-----
 - Loopback-----
 - VLANs (802.1Q e trunk) -----
 - Software switch -----
- Routing estático e baseado em políticas (PBR - Policy Based Routing)-----
- SD-WAN-----



- Application Awareness & Steering (3000+ Applications Supported)-----
- Dynamic WAN Path Controller -----
- NGFW with SSL Inspection-----
- Dynamic failover times -----
- Secure VPN Overlays -----
- Single Management Console for Security & SD-WAN-----
- Zero-touch provisioning-----
- Balanceamento e redundância de múltiplos links;-----
- Suporte para protocolos de routing dinâmico: RIPv2, RIPv6, OSPFv2 e OSPFv3, ISIS, BGP4+-----
- Suporte de tráfego multicast: PIM, sparse e dense mode-----
- Routing baseado em conteúdos: WCCP e ICAP -----
- Proxy explícito com suporte PAC e WPAD-----
- Suporte de IPv6 -----
 - Gestão por IPv6-----
 - Protocolos de routing dinâmico com suporte para IPv6 -----
 - Tunneling de IPv6-----
 - Processamento firewall e UTM de IPv6 -----
 - NAT64-----
 - NAT46-----
 - VPN IPSec IPv6-----
- Suporte Dual Stack IPv4 e IPv6 em simultâneo -----
- Suporte VXLAN -----
- Controlador Wireless integrado -----
- Controlador Switching integrado -----
- Virtualização da solução em contextos -----

Identificação de utilizadores e dispositivos-----

As seguintes funcionalidades deverão ser suportadas: -----

- Base de dados local de utilizadores;-----



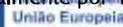


- Autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+ -----
- Sistema de Single Sign-on de utilizadores: -----
 - Windows AD-----
 - Kerberos-----
 - Novell eDirectory -----
 - Citrix e Terminal Server-----
 - Radius (accounting message) -----
 - Autenticação de utilizadores no acesso (802.1x, portal cativo) -----
- PKI e certificados:-----
 - Certificados X.509-----
 - Suporte SCEP-----
 - Criação de Certificate Signing Request (CSR)-----
 - Auto renovação de certificados antes da data de expiração-----
 - Suporte OCSP -----
- Autenticação de 2 fatores -----
 - Servidor integrado de autenticação por tokens físicos, tokens por software e SMS-----
 - Integração com terceiras partes -----
- Identificação de dispositivos (incluindo dispositivos IoT)-----
 - Reconhecimento de dispositivo e sistema operativo -----
 - Classificação automática de dispositivos-----
 - Gestão de inventário de dispositivos -----
 - Suporte de autenticação e bypass feitos por MAC Address-----
- Implementação de políticas de segurança com base em utilizador ou dispositivos -----

Firewall-----

As seguintes funcionalidades deverão ser suportadas: -----

- Modos de operação NAT/route e transparent/bridge -----
- Agendamento de políticas: recorrentes ou apenas uma vez -----





- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, RTSP, SIP, TFTP, GTP-C, GTP-U, GTP-B, TNS (Oracle) -----
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pinhole -----
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP -----
- Visualização de políticas de forma global ou por pares de interfaces -----
- Definição de objetos para utilização em políticas incluindo: pré-definidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos -----
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia e FQDN -----
- Utilização de objetos de serviços Internet (ex: Azure, Office365) com atualização automática das gamas de IP e portos. -----
- Configuração de NAT: por política e tabela central de NAT -----
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT, STUN ---
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ) -----
- Processamento de tráfego de firewall IP4 e IPv6 feito em processador dedicado e desenhado para o efeito. -----

VPN-----

As seguintes funcionalidades deverão ser suportadas: -----

- IPSEC VPN:-----
 - Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico -----
 - Mecanismos de autenticação: certificados ou pre-shared key -----
 - IPSEC Phase 1 mode: aggressive e main (ID protection) mode -----
 - Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup -----
 - Suporte de IKEv1, IKEv2 (RFC 4306) -----



- Suporte de IKE mode configuration (como servidor ou cliente), DHCP over IPSEC-----
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256-----
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512 -----
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14 -----
- Suporte XAuth como cliente ou servidor-----
- XAuth para clientes dialup: Server type option (PAP, CHAP, Auto), NAT Traversal option
- Duração configurável da chave de encriptação IKE e da frequência do NAT traversal keepalive -----
- Dead peer detection -----
- Replay detection -----
- Autokey keep-alive na Phase 2 SA -----
- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente-----
- Suporte ADVPN -----
- Suporte de configuração full-mesh VPN One-click-----
- Opções de configuração de VPNs IPSec: baseado em routing (route-based) ou baseado em políticas (policy-based)-----
- VPNs SSL -----
 - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente -----
 - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
 - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos -----
 - Gestão de atalhos (bookmarks) pessoais -----
 - Gestão de utilizadores concorrentes -----
 - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
 - Suporte de VPN SSL em modo web: -----
 - Para clientes remotos equipamentos apenas com um browser web-----



- Disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix -----
- Suporte para VPN SSL em modo túnel:-----
 - Para acesso a partir de computadores que necessitam utilizar qualquer software do tipo cliente-servidor. -----
 - Disponível para MAC OSX, Windows, IOS, Android e Windows Mobile -----
- Suporte para VPN SSL em modo port-forwarding: -----
 - Utiliza uma applet Java para permitir uma utilização alargada de aplicações do tipo cliente-servidor-----
- Validação da integridade do dispositivo cliente e do sistema operativo;-----
- Opção para limpeza de cache aquando do termino da sessão VPN SSL -----
- Opção de utilização de desktop virtual que permite isolar a sessão VPN SSL no ambiente de trabalho do computador cliente-----
- Monitorização de VPNs IPSec e SSL com diferentes níveis de detalhe-----
- Suporte para outras VPNs como L2TP (modo cliente e servidor), L2TP over IPSec, PPTP e GRE over IPSec -----
- Processamento de tráfego de IPSec feito em processador dedicado e desenhado para o efeito.-----

IPS - Detecção e prevenção de intrusões-----

As seguintes funcionalidades deverão ser suportadas: -----

- Suporte de IPS com mais de 12000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados-----
- Diferentes ações de IPS: monitorizar, bloquear, apagar sessão ou quarentena do IP de ataque com definição de duração -----
- Possibilidade de registo integral do pacote onde foi detetado o ataque-----





- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo) -----
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade -----
- Opção de excluir a aplicação de assinaturas de IPS específicas com base em IPs -----
- Proteção DoS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)-----
- Possibilidade de implementação de IDS em modo sniffer -----
- Possibilidade de criar novas assinaturas-----
- Possibilidade de incluir assinaturas específicas para proteção de comunicações e equipamentos em ambientes industriais-----

Controlo de aplicações-----

As seguintes funcionalidades deverão ser suportadas: -----

- Detecção de mais de 3100 aplicações distintas organizadas por categorias-----
- Definição de aplicações customizadas -----
- Controlo avançado de aplicações de IM e Facebook -----
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco e/ou protocolo) -----
- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade-----
- Detecção de aplicações mesmo dentro de ligações proxy -----
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização ou aplicação de gestão de largura de banda-----
- Inspeção SSL (suporte TLS 1.3)-----

Proteção contra ameaças-----

As seguintes funcionalidades deverão ser suportadas: -----

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, web filtering e DLP -----





- Capacidade de descriptação de sessões SSL com cópia de tráfego descriptado para um sistema externo-----
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MITM -----
- Detecção e bloqueio de BOTNETs com base em listas de reputação de IPs globais; -----
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores -----
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTSP, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP -----
- Suporte de anti-vírus em modo proxy, incluindo:-----
 - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTSP, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP -----
 - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)-----
 - Listas de ficheiros autorizados/negados -----
 - Opção de análise heurística -----
- Integração com solução de Sandboxing (cloud ou on-premises)-----
- Detecção de sites WEB (web filtering):-----
 - Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS) -----
 - Possibilidade de definição manual de filtros de sites com base em URL, conteúdo web e cabeçalho MIME -----
 - Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias-----
 - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter-----
 - Deverá ser possível ter a opção para activar as seguintes funcionalidades: -----
 - Filtrar Java Applet, ActiveX e/ou cookies-----
 - Bloquear HTTP Post-----



- Registrar termos/palavras utilizados nas pesquisas em motores de busca-----
- Identificar imagens pelo URL-----
- Bloquear redirect de HTTP de acordo com a categoria-----
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores-----
- Definição de quotas de utilização WEB com base em categorias -----
 - Definição de categorias customizadas e sobreposição de categorização-----
 - Mecanismos de exceção à utilização de perfis pré-definidos;-----
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Prevenção e proteção de fugas de informação – DLP-----
- Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP-----
- Possibilidade de executar as acções: registar, bloquear, quarentena de utilizador/IP/Interface-----
- Filtros pré-difinidos incluindo cartões de crédito e número de segurança Social-----
- Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP-----
- Opções de filtro disponíveis: tipo de ficheiro, watermark, conteúdo e deteção de encriptação -----
- Utilização de mecanismos de DLP watermarking , com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux -----
- Fingerprinting de ficheiros -----
- Armazenamento de ficheiros detetados para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB -----
- Integração nativa com plataformas externas de filtragem de email, sandbox e WAF -----
- Feeds de ameaças por Domain Name e/ou IP Address -----



Controlo de equipamentos terminais-----

- Visibilidade centralizada sobre diversos elementos de rede, nomeadamente:-----
 - Vulnerabilidades nos equipamentos terminais-----
 - Indicadores de compromisso -----

Alta disponibilidade -----

As seguintes funcionalidades deverão ser suportadas: -----

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes -----
- Interfaces reservadas para gestão -----
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade-----
- Reposição automática de serviço (failover)-----
 - Monitorização de portas e links (locais e remotos) -----
 - Sem perda de sessões-----
 - Failover em menos de 1 segundo-----
 - Notificações de eventos de failover-----
- Diferentes opções de arquitetura -----
 - HA com agregação de links-----
 - Full mesh HÁ-----
 - Suporte para HA com equipamentos geograficamente dispersos-----
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico-----

Administração, Monitorização e Diagnósticos -----

As seguintes funcionalidades deverão ser suportadas: -----

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser-----
- Acesso de gestão em modo de texto: SSH, Telnet ou consola -----
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica-----



- Suporte para gestão local e gestão centralizada em simultâneo -----
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow -----
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts -----
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades. -----
- Integração com outras soluções (externas) através de scripts CLI e APIs. -----
- Wizards de configuração para implementação rápida da solução. -----
- Integração com soluções Openstack, VMWare NSX, e Cisco ACI. -----
- Automação, por exemplo para colocar em quarentena um dispositivo com um elevado Indicador de Compromisso. -----

Registo de eventos e relatórios -----

As seguintes funcionalidades deverão ser suportadas: -----

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória, disco rígido local, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud -----
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195) -----
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas; -----
- Possibilidade de exportar relatórios em formato PDF -----
- Calendarização de backups de logs para sistemas externos -----
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos -----
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless -----



- Opção para registo parcial ou completo de eventos -----
- Resolução de nomes de endereços IPs e protocolos -----
- Mecanismo nativo de visualização de eventos de forma estatística, com ferramentas de busca e drill-down disponível através de recurso com web browser. -----

b) nível do Acesso sem fios: -----

Access Points do fabricante Fortinet, modelo FAP-231F, ou equivalente (54 Unidades)-----

Pretende-se que os equipamentos a fornecer para a componente de rede de acesso sem fios sejam access points que apresentem as seguintes características técnicas:-----

Requisitos de Conectividade:-----

- 2 Interfaces GE RJ45 10/100/1000 Base-T -----
- 1 Interface USB -----
- 1 Interface RS-232 RJ45 Serial-----

Requisitos de Sistema:-----

- Access points do tipo indoor-----
- Número de rádios: 3 + 1BLE (Bluetooth Low Energy) -----
- Número de antenas: 3 Dual Band Internal Wi-Fi + 1 BLE/Zigbee -----
- Tipo de antena: PIFA (Planar Inverted-F antenna) -----
 - Dual Band: 4.5 dBi for 2.4 GHz, 5.5 dBi for 5 GHz-----
 - BLE: 4.0 dBi at 2.4 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-----
- Capacidade do Radio 1: Frequência: 2.4 GHz-----
 - 20/40 MHz-----
 - BPSK, QPSK, QAM64, QAM256 e QAM1024 -----
 - 2x2 MIMO-----
- Capacidade do Radio 2: Frequência: 5 GHz -----
 - 20/40/80MHz -----

ESEnfc_Mar03-2020





- BPSK, QPSK, QAM64, QAM256, e QAM1024-----
- 2x2 MIMO-----
- Capacidade do Radio 3: Frequência: 2.4 GHz e 5 GHz-----
- 1x1 MIMO-----
- Power over Ethernet (PoE) 802.3at PoE default-----
- 1 interface alimentada pelo standard 802.3at, com suporte de todas as funcionalidades juntamente com a interface USB -----
- 1 interface alimentada pelo standard 802.3af, sem suporte da interface USB -----
- Suportar no mínimo 10 SSIDs simultâneos-----
- Suporte de modo LED desligado-----

Requisitos de Monitorização do espectro rádio:-----

- Capacidade de analisar o espectro rádio-----
- Modo de scan de Rogue APs-----
- Modo de sniffer de tráfego -----

Requisitos de Energia e Alimentação-----

- Alimentação AC: 802.3at PoE para todas as funcionalidades -----
- Consumo de energia máximo: 17W-----
- Temperatura de funcionamento entre os 0 e os 50 °C-----
- Humidade entre os 5% e os 90% sem condensação -----
- MTFB (Mean Time Between Failures) maior do que 10 anos -----

Requisitos de Gestão e Operação:-----

As seguintes funcionalidades deverão ser suportadas:-----

- Configuração através da função de controlador wireless do Sistema de Segurança (firewall)
- Modo de funcionamento Remote VPN tunnel-----



- Descoberta automática de Controladores de Equipamentos Wi-Fi e efetuar o download de configurações para instalações plug-and-play -----
- Protocolo SNMP -----
- Gestão por via de uma plataforma 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-----
- Upgrade ao equipamento a partir da consola de gestão centralizada -----

Requisitos de Segurança:-----

Os equipamentos deverão permitir: -----

- Controlo de acesso por autenticação WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, 802.11i, 802.1X (EAP-TLS, EAP-TTLS, PEAP, EAP-SIM, EAP-AKA, EAP-FAST)-----
- Efetuar o controlo de acesso por autenticação 802.1X e através de um portal (captive portal), sobre uma base de dados local, RADIUS e Active Directory -----
- Controlo de acesso RADIUS por utilizador e ESSID, através de filtragem MAC -----
- Configuração de várias Preshared Keys (Multiple PSK) no mesmo SSID do tipo WPA Personal, bem como definir o número de clientes concorrentes que se podem conectar com cada uma das chaves -----
- Quando gerido pelo sistema de segurança, o equipamento deverá ter a capacidade detetar e classificar dispositivos, e colocá-los em quarentena -----

Requisitos Wireless: -----

Os equipamentos deverão:-----

- Implementar as normas IEEE 802.11 a/b/g/n/ac/ax-----
- Implementar MIMO 2x2 (triple-stream)-----
- Permitir débitos otimizados através de Automatic Radio Resource Provisioning (ARRP)





- Permitir a implementação do protocolo Hotspot 2.0 -----

c) Power Injectors -----

54 Power Injectors compatíveis com o modelo de access points especificado -----

Os equipamentos a fornecer devem ser compatíveis com o modelo de *access points* especificado anteriormente, e neste pressuposto devem suportar os *standards* PoE 802.3af (PoE) e 802.3at (PoE+)

Os equipamentos deverão possuir 2 interfaces *ethernet* 10/100/1000 Mbit/s, uma para ligação ao *access point* e outra para ligação ao *switch* responsável pela comutação de tráfego e interface com a rede local. -----

Lote 10.2 - Software, licenciamento e suporte -----

O licenciamento do software de todos os equipamentos a considerar neste procedimento deve ser efetuado em nome da entidade adjudicante. -----

Futuras versões do software para os equipamentos a fornecer terão de ser fornecidas sem quaisquer encargos adicionais, durante a vigência do contrato. São consideradas futuras versões software as que corrijam erros ou falhas da versão em utilização, bem como a disponibilização de novas funcionalidades. Nas novas versões de software não poderão ser descontinuadas quaisquer funcionalidades que se encontrem em operação ou previstas neste contrato. -----

Todos os equipamentos deverão ser propostos com todo o licenciamento de software necessário à implementação da solução pretendida por um período mínimo de 3 anos. -----

Não se considera necessário, no âmbito deste procedimento, o fornecimento de licenciamento associado a funcionalidades de segurança avançada relativamente aos equipamentos de segurança. Por funcionalidades de segurança avançada entende-se mecanismos tipicamente associados à camada aplicacional Antivirus, Anti-malware, Intrusion Prevention, Web Filtering. -----



Relativamente à componente de suporte ao hardware contemplado na proposta, pretende-se que a mesma seja garantida durante um período mínimo de 3 anos. Entende-se por suporte ao hardware o acesso direto ao suporte do fabricante para abertura de casos relativamente à operacionalidade da solução, bem como a substituição de equipamentos em caso de avarias. -----

NOTA: Todo o equipamento deve ser novo, não se aceitando equipamentos recondicionados -----

Artigo 19º | Preço

O preço a pagar de acordo com o lote adjudicado é no montante de 71 955,24€ (setenta e um mil novecentos e cinquenta e cinco euros e vinte e quatro cêntimos). -----

Valor acrescido de IVA à taxa legal em vigor. -----

Artigo 20º | Gestor do contrato

Ao abrigo do art. 290º-A do CCP foi designado gestor do contrato de acordo a [REDACTED] -----

Artigo 21º | Disposições finais

1. A Direção da Escola reserva-se o direito de, junto do adjudicatário, exercer ações de verificação do cumprimento do contrato, nomeadamente, no que respeita à qualidade. -----
2. As dúvidas e casos omissos que eventualmente se suscitarem serão supridos por despacho do Órgão de Direção da Escola, tendo subjacente a legislação aplicável à matéria em causa. -----
3. Em tudo o omissos neste Caderno de Encargos observar-se-á a legislação aplicável. -----
4. Os pagamentos ao abrigo do presente contrato serão efetuados após a verificação dos formalismos legais em vigor para o processamento das despesas públicas e por transferência bancária. --



5. Ao abrigo do nº 1 do art.º 94º do CCP o presente contrato é elaborado em suporte informático, constituído por vinte e oito folhas, numeradas, com aposição de assinaturas eletrónicas das partes.
6. O contrato será suportado por conta das verbas inscritas no orçamento da Escola ESEnFC, sob as rubricas orçamentais com as Classificações Económicas: 070107 – Equipamento Informático, 020121 - Outros bens e 060202 - Ativos incorpóreos.-----

O Primeiro Outorgante,

O Presidente da ESEnFC,

(Prof. Doutor António Fernando Salgueiro Amaral)

O Segundo Outorgante,

(Hélder Miguel Ferreira Henriques)