Assinado por : **PAULO SÉRGIO RIBEIRO NOGUEIRA FERRAZ**
Num. de Identificação: BI110692586
Data: 2020.07.15 13:14:01 Hora de Verão de GMT

CARTÃO DE CIDADÃO

FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Caderno de Encargos

"Aquisição de Infraestruturas de acesso 100 Gbps edge, core e segurança de centro de dados para o campus da Universidade de Trás-os-Montes e Alto Douro (UTAD)"

GOVERNO DE PORTUGAL | MINISTRO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

Lisb@20[20] CRESC ALGARVE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

ARTIGO 1.º

OBJECTO

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar entre a Fundação para a Ciência e a Tecnologia, I.P. e adjudicatário na sequência da adjudicação no âmbito da consulta para aquisição de infraestruturas acesso 100 gbps, edge, core e segurança de centro de dados para o campus da Universidade de Trás-os-Montes e Alto Douro (UTAD).

2. O **CONTRATO** a celebrar integra, para além do clausulado contratual:

a) os suprimentos dos erros ou 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, nos termos do artigo 50º do Código dos Contratos Públicos;

b) os esclarecimentos e retificações relativos ao caderno de encargos que sejam emitidos ao abrigo do artigo 50º do Código dos Contratos Públicos;

c) o caderno de encargos;

d) a proposta adjudicada;

e) os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3. Em caso de divergência entre os documentos referidos nas diferentes alíneas do número anterior, a prevalência obedece à ordem por que vêm enunciados nas suas diferentes alíneas.

4. Em caso de divergência entre os documentos referidos nas diferentes alíneas do nº 2 e o clausulado contratual, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101º do mesmo diploma.

ARTIGO 2.º

OBRIGAÇÕES DO ADJUDICATÁRIO

1. O adjudicatário obriga-se a executar o Contrato em termos que se conformem com o estabelecido no Caderno de Encargos, nos anexos que dele fazem parte integrante e na legislação aplicável.
2. Para além de outras obrigações previstas na lei ou no presente caderno de encargos, o adjudicatário obriga-se a:

    a) Assegurar que o objeto da prestação obedece às especificações técnicas exigidas;
    b) Obrigação de manutenção;
    c) Cumprir os prazos estabelecidos, designadamente, para a execução das prestações a que se obriga;
    d) Prestar informação;

e) Assegurar o sigilo.

ARTIGO 3.º

ESPECIFICAÇÕES TÉCNICAS

O adjudicatário obriga-se a assegurar que o objeto de aquisição obedece às especificações técnicas que constam do Anexo I ao presente Caderno de Encargos, do qual faz parte integrante.

ARTIGO 4.º

PRAZOS

O adjudicatário obriga-se ao pontual cumprimento de todos os prazos de execução das prestações objeto do contrato, os quais são os que constam do clausulado deste, da proposta do adjudicatário ou de outros documentos referidos no nº 2 do artigo 1º.

ARTIGO 5.º

ENTREGA

1. Os bens objeto de adjudicação consideram-se entregues após a respetiva aceitação por parte da FCT, I.P, a qual será comunicada por escrito ao adjudicatário.

2. O adjudicante poderá promover a realização de testes de aceitação, destinados à verificação da conformidade dos bens objeto de adjudicação com os requisitos técnicos constantes do presente Caderno de Encargos.

3. Os testes referidos no número anterior devem ocorrer no prazo de 21 (vinte e um) dias corridos após a receção de todos os bens objeto do contrato a qual deve ocorrer nas instalações da UTAD, sitas em Quinta de Prados, 5001-801 Vila Real no prazo máximo de 28 (vinte e oito) dias corridos contados a partir da entrada em vigor do contrato

4. Os bens consideram-se aceites na data em que a FCT, I.P. disso expressamente notificar, por escrito, o adjudicatário ou, na ausência de notificação, no dia subsequente ao fixado no número anterior como limite para a realização de testes de aceitação.

5. Se nos termos dos testes de aceitação a FCT, I.P. constatar que os bens não cumprem os requisitos técnicos constantes do presente Caderno de Encargos, disso dará conhecimento ao adjudicatário, abrindo-se um prazo de 7 (sete) dias corridos para que este desenvolva as diligências necessárias a que aqueles requisitos sejam cumpridos, e o equipamento seja de novo submetido a testes.

6. Se, estes testes de aceitação, não forem concluídos com êxito, persistindo a desadequação aos requisitos técnicos exigidos, a FCT, I.P. poderá conceder ao adjudicatário novo prazo de 7 (sete) dias corridos para que este desenvolva novas diligências para que os bens cumpram os requisitos do Caderno de Encargos ou, em alternativa, considerar incumprida a obrigação de fornecimento e rescindir o Contrato.

ARTIGO 6.º

OBRIGAÇÃO DE MANUTENÇÃO

Caso se verifique qualquer anomalia no bem objeto de adjudicação que impeça ou prejudique o desempenho da sua função, o adjudicatário obriga-se a proceder, sem custos adicionais para o adjudicante, às operações necessárias à reposição deste nas mesmas condições que deram origem à aceitação nos termos e condições referidas no Anexo I ao presente Caderno de Encargos.

ARTIGO 7.º

OBRIGAÇÃO DE PRESTAÇÃO DE INFORMAÇÃO

O adjudicatário obriga-se a prestar à FCT, I.P.**,** por escrito, toda a informação que lhe for solicitada relativa ao objeto da adjudicação ou à sua atuação em cumprimento das obrigações que para si decorrem do contrato.

ARTIGO 8.º

OBRIGAÇÃO DE SIGILO

O adjudicatário obriga-se a não divulgar informações que obtenha em virtude da execução do **CONTRATO** durante a vigência deste e por um período de dois anos contados a partir da data da sua cessação.

ARTIGO 9.º

PREÇO E CONDIÇÕES DE PAGAMENTO

1. O preço base da aquisição a que se refere o presente caderno de encargos, entendido como o preço máximo que a FCT, I.P. se dispõe a pagar fornecimento dos bens que constituem o seu objeto é de **178.000,00 € acrescidos de IVA** à taxa legal em vigor, dividido por lotes do modo seguinte:

a. Lote 1 – **€ 28.000,00**

b. Lote 2 – **€ 150.000,00**

2. Pela aquisição dos bens objeto da presente aquisição, a FCT, I.P. pagará ao adjudicatário o valor indicado na proposta, acrescido de IVA à taxa legal em vigor, nos termos do número seguinte.

3. A quantia prevista no número anterior deve ser satisfeita através do pagamento de uma fatura, emitida, após a entrega dos bens nos termos a que se refere o artigo 5º.

4. A fatura a emitir pelo adjudicatário assume a forma de fatura eletrónica, com os requisitos legais, nomeadamente os resultantes do artigo 299º-B do CCP.

5. A fatura referida no número anterior será paga no prazo máximo de trinta dias a contar da sua receção.

ARTIGO 10.º

VIGÊNCIA DO CONTRATO

1. O **CONTRATO** inicia a sua vigência na data da respetiva assinatura.

2. O **CONTRATO** cessa vigência no prazo de cinco anos[1] .

3. O artigo 8º cessa vigência na data em que cesse o prazo nele previsto.

ARTIGO 11.º

RESPONSABILIDADE DO ADJUDICATÁRIO

1. O adjudicatário responde pelos danos que causar à **FCT, I.P.** em razão do incumprimento culposo das obrigações que sobre ele impendam, nos termos das normas gerais de direito e do presente artigo.

2. O adjudicatário responde ainda perante a **FCT, I.P.** pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do **CONTRATO**, como se tais atos ou omissões fossem praticados por aquele.

3. O adjudicatário responde, independentemente de culpa, pelos danos causados à **FCT, I.P.** pela execução deficiente do **CONTRATO**.

4. Nenhuma das partes responde por danos causados à outra parte em virtude de incumprimento de obrigações emergentes do **CONTRATO** decorrente de caso fortuito ou força maior.

5. A parte que pretenda beneficiar-se do regime acolhido no número anterior deve, para o efeito, informar a outra parte da verificação de uma situação de incumprimento decorrente de caso fortuito ou de força maior, fazendo menção dos factos que, em seu entender, permitem atribuir esta origem ao incumprimento e, ainda, do prazo que estima necessário para cumprir a obrigação em causa.

ARTIGO 12.º

[1] A vigência do contrato de cinco anos é justificada pela criticidade do equipamento em causa que justifica uma continuidade e estabilidade na sua manutenção durante o período de vida útil do equipamento, que é de cinco anos.

CLÁUSULA PENAL

Pelo incumprimento, sob a forma de mora, de obrigações emergentes do contrato, a **FCT, I.P.** pode, sem prejuízo do n.º 4 do artigo anterior, exigir do adjudicatário o pagamento de uma pena pecuniária no valor de **0,5%** do valor do **CONTRATO** por cada dia de atraso relativamente ao plano de execução previsto para implementação da solução.

ARTIGO 13.º

RESCISÃO

1. A FCT, I.P. pode rescindir o **CONTRATO**:

a) quando, estando o adjudicatário em mora, este não realize a prestação no prazo que lhe haja razoavelmente sido fixado pela FCT, I.P.;

b) com fundamento em incumprimento das obrigações previstas no artigo 2º que determine a perda objetiva de interesse nas prestações que constituam o seu objeto;

2. A rescisão do **CONTRATO** ao abrigo do disposto no número anterior determina a perda da caução prestada pelo adjudicatário, caso esta tenha sido prestada nos termos da lei e a extinção dos créditos de que este seja titular em virtude do referido **CONTRATO**.

3. A perda da caução ao abrigo do número anterior não extingue o direito da **FCT, I.P.** de ser ressarcida da totalidade dos danos que lhe hajam sido causados pela conduta do adjudicatário que haja fundamentado a rescisão.

ARTIGO 14.º

DESPESAS

Correm por conta do adjudicatário todas as despesas em que este haja de incorrer em virtude do cumprimento de obrigações emergentes do **CONTRATO**.

ARTIGO 15.º

LEI APLICÁVEL

O **CONTRATO** rege-se pela lei portuguesa.

ARTIGO 16.º

INTERPRETAÇÃO DO CONTRATO

1. Em caso de dúvida sobre a interpretação das regras aplicáveis à execução do **CONTRATO**, o adjudicatário deve solicitar por escrito um esclarecimento à **FCT, I.P.**.

2. O adjudicatário obriga-se a ter em conta as orientações que lhe forem transmitidas por escrito pela **FCT, I.P.**, na medida em que as mesmas não colidam com as regras aplicáveis à execução do **CONTRATO**.

ARTIGO 17.º

COMUNICAÇÕES

1. Para efeitos de comunicações relativas à fase de execução do contrato, as partes podem recorrer aos seguintes meios de comunicação:

a) correio postal, através de carta registada ou de carta registada com aviso de receção;

b) correio eletrónico;

c) outro meio de transmissão eletrónica de dados.

2. Todas as comunicações devem ser escritas e redigidas em língua portuguesa.

3. Para efeitos de estabelecimento das comunicações a que se refere o presente artigo, as partes identificam os seguintes contactos, através dos quais as mesmas se devem concretizar:

a) Pela FCT, I.P.:

Nome do representante:

Endereço postal: Av. do Brasil, 101 1700-066 Lisboa

Endereço electrónico:

Número de fax:

Para questões de funcionamento e operação dos equipamentos na UTAD:

Nome do representante: António Rio Costa

Endereço postal: Serviços de Informática e Comunicações, Edifício de serviços comuns, Quinta de prados, 5001-801 Vila Real

Endereço eletrónico: sic_ics@utad.pt

b) Pelo adjudicatário:

Nome do representante:

Endereço postal:

Endereço eletrónico:

Número de fax:

ARTIGO 18.º

GESTOR DO CONTRATO

Para o exercício das funções de acompanhamento da execução do contrato nos termos regulados pelo artigo 290º-A do Código dos Contratos Públicos é designado António Manuel Araújo da Silva Rio Costa, Especialista de Informática da Universidade de Trás-os-Montes e Alto Douro.

ARTIGO 19.º

CESSÃO DA POSIÇÃO CONTRATUAL

1. A cessão da posição contratual do adjudicatário é possível nos termos do artigo 318º do Código dos Contratos Públicos.
2. Em caso de incumprimento contratual pelo adjudicatário que seja suscetível de conduzir à resolução do contrato, a sua posição contratual pode ser cedida aos concorrentes do procedimento pré-contratual classificados nas posições subsequentes à do adjudicatário, nos termos do estabelecido no artigo 318º-A do Código dos Contratos Públicos.

ARTIGO 20.º

DADOS PESSOAIS

1. No tratamento de dados pessoais por conta do adjudicante, o adjudicatário obriga-se ao escrupuloso cumprimento do Regulamento Geral sobre a Proteção de Dados (Regulamento 2016/679) e demais legislação aplicável.
2. O tratamento referido no número anterior é apenas o necessário à execução do contrato e feito durante a sua vigência, aplicando-se, em especial, o estabelecido no nº 3 do artigo 28º do Regulamento Geral sobre a Proteção de Dados.

ARTIGO 21º

(ASSINATURA DO CONTRATO)

O contrato a celebrar entre a FCT, I.P. e o adjudicatário será celebrado com recurso preferencial, por ambas as partes, à assinatura eletrónica qualificada, tal como definida pelo Decreto-lei nº 290D/99, de 2 de agosto, com as alterações introduzidas pelos Decretos-lei n.º 62/2003, de 3 de abril, 165/2004, de 6 de julho e 116-A/2006, de 16 de junho.

ARTIGO 23.º

(TRIBUNAL DE CONTAS)

1. O contrato poderá estar sujeito a fiscalização prévia do Tribunal de contas, nos termos do disposto nº 2, do artigo 318.º da LOE 2020, conjugado com o nº 2 do artigo 48.º da Lei de Organização e Processo do Tribunal de Contas, na sua redação atual
2. Caso se verifique o previsto no número anterior, o contrato apenas produz efeitos financeiros a partir data de obtenção do referido Visto;
3. Os emolumentos devidos, no valor legal, serão suportados pelo adjudicatário.

ANEXO I

Especificações técnicas

Infraestrutura de acesso 100Gbps edge, core e segurança de centro de dados

Este documento contém as especificações técnicas aplicáveis ao fornecimento de equipamentos e sua instalação com vista à implementação nas instalações da Universidade de Trás-os-Montes e Alto Douro (UTAD), no âmbito do projeto RCTS100, de interligação das entidades de ensino superior em rede de alto débito.

Cofinanciado por:
COMPETE 2020
Lisb@20^20
CRESC ALGARVE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Lote 1 – Equipamentos de Core/Edge com conetividades de 10 a 100 Gbps

1 INTRODUÇÃO

O adjudicatário compromete-se a fornecer uma solução de 1 (um) equipamento de core/edge com funcionalidades de L2/L3 de acordo com características técnicas mínimas seguidamente descritas.

Esta solução deve integrar com a solução e infraestruturas já existente na UTAD, permitir a gestão centralizada que terá a capacidade de agregação e análise integrada de rede.

2 REQUISITOS EQUIPAMENTO

2.1 EQUIPAMENTOS DE CORE/EDGE

Quantidade a fornecer: 1 (um).

2.1.1 Características

- Características Físicas;
- Equipamento fixo Ethernet L2/L3;
- Dimensões: 1RU;
- 24 portas 1/10/25G SFP+ mais 4 portas 40/100G;
- Suporte dos seguintes óticos do tipo QSFP+ :
    - 40GBASE-SR4, 40GBASE-LR4, 40GBASE-ER4;
- Suporte dos seguintes óticos do tipo QSFP28 :
    - 100G-SR4, 100G-LR4, 100G-ERL4;
- Suporte dos seguintes óticos do tipo SFP+:
    - 10G Base SR, 10G Base LR, 10G Base LRM, 10G Base ER, 10G Base ZR;
- Suporte dos seguintes óticos do tipo SFP:
    - 1000Base T, 1000Base SX, 1000Base LX/LH, 1000Base EX, 1000Base ZX;
- Suporte de flash com um mínimo de 16GB para guardar configurações e logs;
- Suporte para fontes de alimentação redundantes;
- Suporte para fans redundantes e hot-swappable;
- Suporte de RFID embebido no equipamento para gestão de activos;
- MTBF Mínimo: 336,780 horas;

2.1.2 Escalabilidade e Performance

- Capacidade de switching mínima: 2.0Tbps;

- Capacidade de forwarding mínima: 1Bpps;
- Número mínimo de VLANIDS: 4094;
- Número mínimo de SVIs: 1000;
- Instâncias de MST: 64;
- Instâncias de (RSTP/PVSTP): 1000;
- Número mínimo de MAC Addresses: 82000;
- Número mínimo de rotas IPv4: 212000;
- Número mínimo de rotas IPv4 multicast: 32000;
- Número mínimo de rotas IPv6 multicast: 32000;
- Número mínimo de rotas IPv6: 32000;
- Número mínimo de entradas ACL: 27000;
- Suporte de 128 Port-Channles com suporte de até 16 membros por port-channel;
- Suporte de Blue Beacon para identificação do switch;
- Packet Buffers de 36M por ASIC;
- Suporte de Jumbo Frames de 9216 bytes;

2.1.3 Funcionalidades

- Suporte para LLDP;
- Suporte de gestão web (HTTPS) embutida no equipamento;
- Suporte de LACP - 802.3ad;
- Suporte para IPv6 em Hardware;
- Suporte de ACLs;
- Suporte de 802.1ad (QINQ);
- Suporte Selective QINQ ou Vlan Mapping;
- Suporte de STP, MSTP;
- Suporte de VRRP;
- Suporte de marcações CoS e DSCP;
- Suporte de WRED, Shaped Round Robin (SRR) e Committed Rate Limit (CIR);
- Suporte de MACSec (802.1AE) com encriptação 256 bits (switch to switch e host to switch);
- Suporte de rotas estáticas IPv4 e IPv6;
- Suporte de RIPv1, RIPv2, RIPnG;
- Suporte de OSPFv2 e OSPFv3;
- Suporte de BGP e IS-IS;
- Suporte de PBR;
- Suporte de MPLS Layer 3 VPNs;
- Suporte de EoMPLS;
- Suporte de H-VPLS;
- Suporte de 6PE e 6VPE;
- Suporte de MPLS Multicast VPN;
- Suporte de VRF-Lite;
- Suporte de VXLAN;

- Suporte de BGP EVPN;
- Suporte de NAT e PAT;
- Suporte de NETCONF, RESTCONF e YANG;
- Suporte para hosting de aplicações third party em containers directamente no equipamento;
- Suporte de Python;
- Suporte de patching para correção de bugs sem necessidade de instalar novas imagens de software;
- Suporte de Port Mirroring e envio de tráfego monitorizado para equipamento remoto através de uma rede Layer3;
- Suporte de Flexible Netflow;
- Suporte de detecção de fluxos ao nível aplicacional - Layer L7, mínimo de 1400 aplicações. Exemplos de aplicações: facebook, skype, yahoo, http, https/ssl, youtube
- Suporte IGMP;
- Suporte de PIM Stub e SSM, DM e SM;
- Suporte de SSHv2;
- Suporte de SNMPv3 e Syslogs;
- Suporte para 802.1X;
- Suporte de funcionalidades de segurança para defesa da integridade do hardware e software do switch, nomeadamente:
    - Assinatura de imagens para garantir a autenticidade da imagem de software;
    - Boot seguro do switch assente em chip de hardware imutável (IEEE 802.1AR).

2.1.4 Terminadores óticos

Quantidades a fornecer:

- 8 (oito) - SFP 10G Base SR;
- 8 (oito) SFP 10G Base LR.
- 4 (quatro) QSFP – 40/100GB -SRBD.

3 OUTROS REQUISITOS

3.1 REQUISITOS GERAIS

- A proposta deverá incluir:
    - Cabos de ligação de energia de todas e fontes redundantes 220V;
    - Cabos de fibra (tamanho previsto de 2,5 metros), com conectores compatíveis e nas quantidades necessárias para suprir todas a ligações possíveis e previstas na proposta;

3.2 SERVIÇOS DE IMPLEMENTAÇÃO, NOMEADAMENTE

- Instalação física dos equipamentos;

- Instalação, arranque e configuração inicial;
- Interligação à rede (Vlans, 802.1q, *Routing*,etc);
- Integração com plataforma unificada de gestão;
- Configuração das políticas de *Firewal*,
- Testes funcionais da solução;
- Apoio à entrada em produção;
- Treino e certificação de técnicos internos (3);
- Documentação do projeto.

4 SUPORTE, MANUTENÇÃO E APOIO TÉCNICO NO LOCAL

- *Back-to-Back* com fabricante com suporte (8X5XNBD), com direito a atualizações de software e assinaturas para 5 anos.

Lote 2 - Solução de segurança redundante

5 INTRODUÇÃO

O adjudicatário compromete-se a fornecer uma solução de *Next Generation Firewall* composta por um cluster de *Appliances* físicas com capacidade para 20 contextos (*firewalls* virtuais) por *Appliance*.

Esta solução deve ter uma plataforma de gestão central de forma a permitir a gestão centralizada e agregação e análise de *Logs.*

6 REQUISITOS GERAIS

a. O adjudicatário deverá endereçar todos os requisitos de um equipamento de segurança (Firewall), tais como processamento de largura de banda, número de ligações, capacidade providenciar segurança a aplicações de nova geração em todas as vertentes da rede (escritório, centro de dados) num único equipamento;
b. O adjudicatário deverá suportar as últimas tecnologias de inspeção avançada *(Firewall, intrusion prevention, application control, URL filtering, Anti-Bot, Anti-Virus, Sandboxing*) em modelo físico e virtual, quaisquer destas geridas por uma única consola central e dedicada;
c. A solução fornecida, deverá suportar (ou vir a suportar através de licenciamento adicional) todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante (single vendor):
    i. *Statefull Inspection Firewall* - A *gateway* deverá inspecionar *end-to-end* (não apenas *half-way* ou *header*) todos os fluxos de comunicação desde o estabelecimento da sessão (3-way *handshake* TCP), durante a transferência de informação (*payload*), até que esta seja terminada;
    ii. *Intrusion Prevention System*;
    iii. *User Identity Acquisition*;
    iv. *Application Control and URL filtering*;
    v. *Anti – Bot / Anti – Virus*;
    vi. *Threat Emulation (Sandboxing)*;
    vii. *Threat Extraction (scrubbing)*;
    viii. *Anti – Spam and Email Security*;
    ix. *IPSec VPN;*

x. *Remote Access VPN (Mobile Access)*;
xi. *Data Loss Prevention*;
xii. *Logging and Status*;
xiii. *Event Correlation and Reporting.*

d. A solução fornecida deverá conter uma plataforma de gestão dedicada de tal modo que:
   i. Haja centralização de políticas, *logs, reports*;
   ii. Não tenha limite de *storage* com base em requisitos de licenciamento;
   iii. O servidor de gestão deverá ter a capacidade de obter detalhes de configuração diretamente das *gateways de firewall* (*fetch* de informação de *routing,* interfaces, etc.) de forma "automática", e não apenas se estas forem instanciadas previamente via *template,* a partir do servidor de gestão.

7 HARDWARE POR *APPLIANCE*

7.1 REQUISITOS FÍSICOS

- HDD redundantes (RAID);
- 64 GB de memória com possibilidade de expansão futura até 128GB;
- Modularidade de interfaces;
  - 5 slots de expansão;
  - Deverá ser flexível quanto o número/tipos de interfaces a aplicar ao chassis:
    - Módulos de 8x1GE UTP (até 40 portas);
    - Módulos de 4x1GE SFP FO (até 20 Portas);
    - Módulos de 4x10FE SFP+ FO (até 20 portas);
    - Módulos de 2x40GE QSFP+ FO (até 6 portas);
    - Módulos de 2x100/25GE QSFP28 FO (até 6 portas);
    - Flexibilidade de combinações com base nos grupos acima descritos;
  - Deverá ser proposto no mínimo as seguintes interfaces:
    - 8x1Gbe em cobre;
    - 10x10Gb SFP+ em fibra e respetivos *transceivers* (10GBase-SR);
    - 2x100Gb QSFP em fibra e respetivos *transceivers* (100GBase-SR);
- Interface LOM (*Lights Out Manager*);
- Interface de gestão dedicada 1x1Gbps cobre;
- Fontes de alimentação redundantes (PSU) AC 90-264V e *Hot swappable*:

- Potência de 800W;
- Consumo máx. aprox. 400W.

7.2 REQUISITOS DE PERFORMANCE

Parâmetro	Métrica
Threat Prevention/Extraction	>=11Gbps
NextGen Firewall	>=13.75Gbps
Intrusion Prevention System	>= 14.45Gbps
VPN Throughput	>= 26Gbps
Firewall Throughput (ideal conditons)	>= 100Gbps
Connections per second	>= 310k
Concurrent Connections	>= 25.6M

8 FIREWALL

8.1 REQUISITOS - FUNCIONALIDADES DE REDE

- Suporte para 1024 interfaces VLAN;
- Suporte para 4096 interfaces VLAN (em cenário de contextos virtuais de *firewall*);
- Suporte para protocolos de agregação de links (LACP 802.3ad);
- Suporte para funcionamento em modo L2 (*bridging*) e L3 (*routing*);
- Suporte de NAT:
  - *Static, Hide, PAT*;
  - NAT44, NAT46, NAT64, NAT66;
- Suporte para *routing* estático;
- Suporte para Policy Based Routing (PBR);
- Suporte para protocolos de *routing* dinâmico:
  - BGP, OSPF (v2 | v3);
  - Suporte para *multicast*;
- *Routing Multicast*:
  - L2 (IGMP v1 | v2);
  - L3 (PIM-SM, PIM-SSM, PIM-DM);

8.2 REQUISITOS DE ALTA DISPONIBILIDADE

- Activo/Passivo ou Activo/Standby
  - VRRP ou IP Virtual;
  - *Failover*:
    - Falhas de *routing*;
    - Falhas de dispositivo;
    - Falhas de link;
  - Sincronização de sessões entre membros do cluster;

8.3 REQUISITOS TÉCNICOS/LÓGICOS

- O equipamento de segurança, deve suportar ***Stateful Inspection***, para construir e manter a tabela de sessões (fluxos de comunicação).
- O equipamento de segurança deve ser capaz de suportar o débito, número de novas ligações e manutenção das mesmas, de acordo com as necessidades do cliente.
- A plataforma de gestão deve permitir visualizar número de acessos por regra.
- A solução tem de suportar a aplicação de regras em intervalos de tempo, para que seja possível definir o tempo útil das mesmas.
- A comunicação entre a firewall e a solução de gestão, tem de ser encriptada e autenticada, com recurso a infraestrutura própria de PKI
- O equipamento de segurança tem de suportar métodos de autenticação por sessão, utilizadores e clientes.
- Os seguintes métodos de autenticação de utilizadores têm de ser suportados pelos módulos de VPN e Firewall:
  - *Tokens (ie -SecureID);*
  - *TACACS;*
  - *RADIUS;*
  - Certificados Digitais.
- A solução tem de ter base de dados de utilizadores local, para permitir a autenticação e autorização dos mesmos sem recurso a um dispositivo externo.
- A solução tem de suportar as funções de DHCP server e *Relay.*
- A solução tem de suportar a função de proxy em HTTP e HTTPS.

- A solução tem de ter capacidade de trabalhar em modo transparente/Bridge (L2)
- A solução tem de suportar alta disponibilidade ou *load sharing* e sincronização de estados entre os dois membros do cluster.

9 SISTEMA DE PREVENÇÃO DE INTRUSÕES (IPS)

- O IPS deve ser baseado nos seguintes mecanismos de deteção:
  - Assinaturas;
  - Anomalias no protocolo;
  - Controlo Aplicacional;
  - Análise de comportamento.

- O administrador deve ter a possibilidade de configurar a inspeção para proteção apenas da rede interna.
- O IPS deve ter opções para criar perfis com base em assinaturas, para proteção de Clientes ou servidores. Também deve ser possível criar um perfil para proteção de ambos.
- O IPS deve fornecer pelo menos dois/duas perfis/políticas predefinidas que podem ser utilizados no *deployment* da solução.
- O IPS deve ter um mecanismo *fail-open* baseado em software, ajustável com base nos limites do *Gateway,* CPU ou utilização de memória.
- O IPS deve ter mecanismo automático para ativar ou gerir as novas assinaturas após atualizações.
- O IPS deve suportar exceções com base na origem, destino, protocolo, ou uma combinação dos três.
- O IPS deve permitir mudar para o modo de deteção, sem alterar parâmetros individuais, por forma a facilitar as ações de *troubleshooting*.
- O IPS deve possuir uma solução centralizada de correlação e relatório de eventos.
- O administrador deve poder ativar de forma automática novas proteções, com base em parâmetros configuráveis:
  - impacto no desempenho;
  - Grau de severidade da ameaça;
  - nível de confiança;
  - proteções do cliente;
  - proteções do servidor.
- O IPS deve ser capaz de detetar e prevenir os seguintes tipos de ameaça:

- uso indevido de protocolo;
- comunicações de *malware*;
- tentativas de uso de protocolos de *tunneling*;
- tipos genéricos de ataque sem assinaturas predefinidas.

- Para cada proteção, a solução deve incluir o tipo de proteção (relativamente a servidor ou cliente):
  - gravidade da ameaça;
  - impacto no desempenho;
  - nível de confiança;
  - referência - (ie CVE);
- O IPS deve ser capaz de capturar pacotes/evidências para proteções específicas.
- O IPS deve ser capaz de detetar e bloquear ataques nas *layers de network* e *application layer*, protegendo pelo menos os seguintes tipos de serviços:
  - Serviços de email;
  - DNS;
  - FTP;
  - Serviços do Windows (Microsoft *Networking*).

- O IPS e/ou o *Aplication Control* deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (*Anonymizers).*
- O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou *hosts*.
- A solução deve proteger DNS Cache *Poisoning* e impedir o acesso dos utilizadores a endereços de domínio bloqueados.
- A solução deve fornecer proteções para protocolos VOIP.
- O IPS e/ou o *Aplication Control* devem detetar e bloquear aplicações que permitam controlo remotos, incluindo as que são capazes de realizar *tunneling* sobre o tráfego HTTP.
- IPS deve ter proteções SCADA.
- IPS deve possibilitar a conversão de assinaturas SNORT.
- A solução deve permitir ao administrador bloquear de forma fácil o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os intervalos de IP correspondentes ao país.

10 AQUISIÇÃO DE IDENTIDADE DE UTILIZADORES (*USER ID ACQUISITION*)

- Deve ser capaz de adquirir a identidade dos utilizadores, com base na consulta dos eventos de segurança da Microsoft *Active Directory.*

- Deve ser possível a autenticação através de uma browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio.
- Deve ter um agente que possa ser instalado nos *endpoints*, para reportar a firewall as identidades dos utilizadores.
- A solução deve integrar-se perfeitamente com Microsoft *Active Directory*, IF-MAP e *Radius*.
- A solução de aquisição de identidade deve suportar soluções de *Terminal server e citrix.*
- A solução deve permitir a identificação de utilizadores que acedem através de um proxy (exemplo: *X-forwarded headers*).
- Deve ser capaz de adquirir a identidade de um utilizador presente numa Microsoft *Active Directory* sem qualquer tipo de agente instalado no controlador de domínio.
- Deve suportar autenticação *Kerberos* para single *sign on.*
- Deve suportar LDAP *nested groups.*
- Deve ser capaz de partilhar identidades de utilizadores entre vários *gateways* de segurança.
- Deve ser capaz de criar *identity roles* (grupos de identidades) para serem invocados em diferentes aplicações da solução.

11 FILTRAGEM DE URL E CONTROLO DE APLICAÇÕES

- A solução deve reconhecer e controlar mais de 6000 aplicações conhecidas.
- A base de dados da solução deve conter mais de 200 milhões de URLs categorizados, abrangendo mais de 85% da Alexas top 1M sites.
- A solução deve permitir a criação de uma regra de filtragem de conteúdos com várias categorias.
- A solução deve permitir filtrar conteúdos de URLs baseada em HTTPS sem efetuar inspeção de SSL.
- A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias.
- A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores.
- A solução deve ter uma interface fácil de pesquisa de aplicações e URLs.
- A solução deve categorizar aplicações e URLs por fator de risco.

- A política de URLF e *Aplication Control* deve poder ser definida por identidade do utilizador.
- A base de dados de URLF e *Application Control* devem ser atualizados por um serviço *Cloud.*
- A solução deve ter o controlo de aplicações e URLF unificado na mesma política.
- A solução deve ter mecanismos para informar ou perguntar ao utilizador em tempo real, para os educar ou para confirmarem as suas ações com base na política de segurança.
- A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda.
- A solução deve permitir exceções com base em objetos de rede previamente definidos.
- A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação.
- A solução deve incluir um mecanismo de *Black e White List*, para permitir que se neguem ou se permitam URLs específicos, independentemente da categoria.
- A solução deve fornecer um mecanismo de substituição na categorização de URL.

12 ANTI-BOT E ANTI-VIRUS

- O adjudicatário deve ter solução de *Anti-Bot e Anti-Virus* integrado na firewall
- A Solução de *Anti-Bot* deve ser capaz de detetar e parar comportamentos de rede suspeitos.
- O aplicativo *Anti-Bot* deve usar um mecanismo de deteção baseado em vários pontos; reputação de endereços IP, URLs e DNS e detetar padrões de comunicação de *bots.*
- A proteção A*nti-Bot* deve ter capacidade de efetuar Scan a ações de *Bot.*
- A solução deve apoiar a deteção e prevenção de vírus e variantes de *Cryptors & ransomware* (por exemplo, *Wannacry, Cryptlocker, CryptoWall* ...) através do uso de análise estática e/ou dinâmica.
- A solução deve ter suporte para proteção contra ataques de *spear phishing*.
- DNS *based attacks* - A solução deve ter recursos de deteção e prevenção para C&C DNS *hideouts*:

    - Pesquisa de padrões de tráfego de C & C, não apenas no destino de DNS.
    - Reverse *engineer do Malware* para descobrir seu DGA (*Domain Name Generation*).
    - DNS Trap, como parte da política de ameaças, interceta e analisa tentativas de comunicações do *endpoint* com C&C.
    - A solução deve detetar e prevenir ataques de DNS *tunneling*.
- A política de *Anti-Bot e Anti-Virus* deve ser gerida a partir de uma consola central.
- A solução de *Anti-Bot e Anti-Virus* deve ter um mecanismo centralizado de correlação e relatório de eventos.
- A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos.
- A solução de antivírus deve poder inspecionar o tráfego SSL.
- O *Anti-Bot e o Anti-Virus* devem ter atualizações em tempo real na *cloud.*
- O *Anti-Virus* deve ser capaz de impedir a entrada de arquivos maliciosos.
- O *Anti-Virus* deve ser capaz de analisar arquivos compactados.
- Políticas antivírus e *Anti-bot* devem ser geridas centralmente e ser possível a parametrização das mesmas.
- O *Anti-Virus* deve suportar a análise de links dentro de emails.
- O *Anti-Virus* deve analisar os ficheiros que passam no protocolo CIFS.

13 IPSEC VPN

- A solução deverá suportar implementações de VPN (*domain based*, e *route based* com protocolos de *routing* dinâmico e virtual *tunnel* interfaces), com utilização de *Internal Certificate Authority ou External 3rd party Certificate Authority*.
- A solução deverá suportar criptografia 3DES e AES-256 para IKE *Phase* 1 e 2.
- A solução deverá suportar criptografia IKEv2 *plus* "Suite-B-GCM-128" e "Suite-B-GCM-256" for IKE Phase 2.
- A solução deverá suportar os seguintes grupos *Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20.*
- A solução deverá suportar os seguintes tipos de mecanismos de integridade de dados:
    - md5;
    - sha1;
    - SHA-256;

- SHA-384;
- AES-XCBC.

- A solução proposta deverá suportar as seguintes funcionalidades VPN:
  - Site-to-site:
    - *Full Mesh* (todos para todos);
    - Estrela (Sites remotos para Site principal);
    - *Hub&Spoke* (Site remotoA para Site RemotoB, através de site principal);
    - Suporte para configuração através de GUI, com opção de *drag&drop* de objetos nas comunidades VPN.
  - Suporte para VPNs de acesso remoto "clientless" e "client based".
  - Suporte para aplicação de políticas de segurança específicas, para controlo de tráfego associado à comunidade VPN.

14 GESTÃO

- A solução deverá possibilitar a segmentação da política de segurança numa estrutura de subpolíticas.
- A solução deverá possibilitar a segmentação da política de segurança numa estrutura de *layers*.
- A solução deverá possibilitar a integração de *logs e audit logs* numa consola única, para contextualizar o administrador ao efetuar alterações sobre a política de segurança.
- A solução de gestão deverá suportar role *based access control*, para segregar acessos de administração para gestão de política e visualização *de logs*.
- A solução deverá implementar um mecanismo de comunicação segura, assente em certificados, entre todas as componentes de segurança integradas no sistema de gestão centralizada.
- A solução deverá incluir um *Certificate Authority x.509* com capacidade para gerir/gerar certificados internos, para autenticação de utilizadores em acessos VPN remotos.
- A solução deverá disponibilizar um mecanismo de pesquisa para facilitar a utilização e identificação de objetos, com base no seu endereço IP.
- A solução deverá disponibilizar métricas de *hit count* nas regras presentes na política de segurança.
- A solução deverá possibilitar a utilização de etiquetas (*labels*) ou secções (*tabs*) para melhor organização da política de segurança.
- A solução deverá permitir gravar a política de forma integral ou parcial.

- A solução deverá disponibilizar um mecanismo de validação da política de segurança, antes da sua instalação nas Gateways de firewall.
- A solução deverá disponibilizar um mecanismo de backup e revisão da política de segurança, possibilitando comparar versões da política e reverter para versões anteriores, se necessário.

15 *LOGGING* E MONITORIZAÇÃO

- A solução de *logging* deverá estar integrada na componente de gestão centralizada, e possibilitar a visualização de *logs* afetos a políticas específicas, sem ser necessário recorrer a uma nova janela, ou aplicação.
- A solução deverá poder ser integrada na componente de gestão centralizada, ou numa *Appliance*/máquina virtual dedicada.
- A solução deverá ter a capacidade de consolidar os *logs* de todas as componentes de segurança que se encontrem ativas na plataforma: IPS, *Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, User Identity, Mobile Access.*
- A solução deverá suportar um mecanismo de captura de pacotes para eventos de IPS, para facilitar despiste e análise forense.
- A solução deverá implementar um mecanismo seguro de *forwarding* de *logs*, com autenticação e encriptação, para evitar potenciais ataques (ex. *Eavesdropping*);
- Os *logs* deverão ser transferidos de forma segura entre a FW *gateway*, o log server e o utilizador final.
- A solução deverá disponibilizar detalhes sobre o estado de todos os túneis IPSEC, site-to-site e *remote access (client-to-site).*
- A solução deverá possibilitar a customização de valores de *threshold*, para execução de ações, uma vez atingido/ultrapassado esse *threshold: log, alert, snmp-trap, email notification.*

16 CORRELAÇÃO DE EVENTOS E *REPORTING*

- A solução deverá integrar a componente de *reporting* e correlação de eventos com a sua componente de gestão centralizada.
- A solução deverá ter a capacidade de correlacionar eventos de todas as funcionalidades ativas nas demais *gateway*s (FW, IPS, URL-F, etc.).
- A solução deverá possibilitar a criação de filtros de *logging,* com base em qualquer característica, tal como: aplicação, ip de origem e destino, serviço, tipo de evento, severidade do ataque, país de origem e destino, etc.

- A solução deverá disponibilizar um mecanismo para assinar os filtros criados a diferentes tipos de gráficos, a serem atualizados periodicamente, apresentando todos os eventos que igualem o filtro aplicado, permitindo ao operador focar-se nos eventos mais importantes.
- A solução deverá assegurar a possibilidade de pesquisar na lista de eventos, e garantir o *drill down* de detalhes em pesquisas e análise forense.
- A solução deverá ter capacidade de detetar e alertar para eventos de login de administradores, em horários não frequentes.
- A solução deverá detetar ataques de *credential guessing / brute force*.
- A solução deverá reportar todos os eventos de alteração/ instalação de políticas de segurança.
- A solução deverá incluir relatórios horários, diários, semanais e mensais predefinidos, incluindo pelo menos: *Top Events, Top Sources, Top Destinations, Top Services,* etc.
- A solução de *reporting* deverá disponibilizar informação consolidada sobre:
    - Volume de ligações bloqueadas por uma regra de segurança em particular;
    - Top de origens bloqueadas, e os destinos e serviços respetivos;
    - Top de regras mais utilizadas na política de segurança;
    - Top de ataques detetados no perímetro, com informação das origens e destinos associados;
    - Atividade web por *user*, com top de web *users* e websites mais utilizados.

17 *SSL INSPECTION (INBOUND / OUTBOUND*)

- A solução deverá suportar inspeção SSL (*inspection/decryption*) com performance comprovada em todas as tecnologias de mitigação.
- A solução deverá suportar *Perfect Forward Secrecy (PFS , ECDHE cipher suites).*
- A solução deverá suportar AES-NI, AES-GCM for *improved throughput*.
- A solução deverá suportar a integração das tecnologias de emulação/*sandboxing* com inspeção SSL.
- A solução deverá permitir a reutilização da base de dados de *URL Filtering*, para criação de políticas de inspeção de SSL granulares.

18 LICENÇAS, SUBSCRIÇÃO

- A nível da plataforma de gestão virtual:
    - Licenciamento perpétuo para 50 ou mais Gateways; (equipamentos/Físicos/Virtuais/ Contextos);

- Subscrição para análise de eventos e *Reporting* para 5 anos.
- A nível das *Appliances* físicas de Firewall:
  - Licença perpétua de Firewall;
  - Licença perpétua para 20 contextos por equipamento;
  - Subscrição de *Anti-Virus, Anti-Bot, IPS, App Control, URL Filtering e Identity Awareness*, para 5 anos.

19 SERVIÇOS DE IMPLEMENTAÇÃO

- Devem ser contemplados serviços de implementação da solução, nomeadamente:
  - Instalação física das *appliances*;
  - Instalação da plataforma de gestão;
  - Interligação à rede *(Vlans, 802.1q, Routing,etc*)
  - Configuração dos 20 Contextos em cada Firewall;
  - Integração dos contextos com a plataforma de gestão;
  - Configuração das políticas de *Firewal, IPS, URL Filtering, Antivírus, e Identity Awareness* em alguns contextos a identificar (estima-se no máximo 2 contextos produtivos);
  - Testes funcionais da solução;
  - Apoio à entrada em produção;
  - Treino e certificação de técnicos internos (3);
  - Documentação do projeto.

20 SUPORTE, MANUTENÇÃO E APOIO TÉCNICO NO LOCAL

- Suporte telefónico e assistência técnica do integrador no local (*on-site*) 8X5xNBD c para 5 anos.
- *Back-to-Back* com fabricante com suporte (8X5XNBD), com direito a atualizações de software e assinaturas para 5 anos.

21 POSSÍVEIS FUTURAS EXPANSÕES E ESCALABILIDADE

A solução deverá permitir acrescentar algumas funcionalidades futuras, através de licenciamentos de “módulos” de software, a saber:

a) Emulação e Extração de Ameaças

- A solução deve ter a capacidade de proteger de ataques desconhecidos *(malware Zero Day*), antes que proteções de assinatura estática sejam criadas:
    - Proteção em Tempo Real para *malware* desconhecido na navegação Web;
    - Proteção em Tempo Real para *malware* desconhecido em email**.**
- Cenários de implementação:
    - A solução deve fazer parte da arquitetura de prevenção de ameaças (com IPS, AV, AB, URLF, APP FW);
    - A solução deve suportar a emulação de ameaças baseada em rede;
    - A solução deve suportar a emulação de ameaças baseada em *host*;
    - A solução deve fornecer solução de implementação *On-Prem e Cloud Based*;
    - Solução de *Cloud* pura;
    - A solução deve suportar integração com *3rd party (public API*);
    - A solução deve suportar implementação em modo *in-line*;
    - A solução deve suportar a implementação modo MTA (*Mail Transfer Agent*);
    - A solução deve suportar implementação em modo de porta TAP / SPAN;
    - A solução não deve exigir infraestrutura separada para proteção email e proteção Web;
    - A solução deve suportar a implementação em modo cluster.
- Tipos de ficheiros Suportados - A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash especificamente:
    - 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, pif, com, gz, bz2, tgz, apk(android), ipa (iphone), ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh.
- A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash, que sejam transmitidos pelos protocolos:
    - HTTP;
    - HTTPS;
    - FTP;
    - SMTP;
    - CIFS (SMB);
    - TLS SMTP.
- OS *support:*

    - O mecanismo de emulação deve suportar vários sistemas operativos, como XP e Windows7, 8,10 32/64 bits, incluindo imagens personalizadas;
    - A solução deve suportar cópias licenciadas de Microsoft Windows e Microsoft Office através de um contrato com a Microsoft;
    - A solução deve detetar chamadas API, alterações em ficheiros, *system registry*, ligações de rede e processos do sistema;
    - A solução deve suportar análise estática para *windows, mac OS-X, Linux* ou qualquer plataforma x86.
- O mecanismo de emulação deve ser capaz de inspecionar, emular, prevenir e compartilhar os resultados do evento de *sandbox* na infraestrutura de *anti-malware.*
- A solução deve permitir a emulação de ficheiros maiores que 10 Mb, em todos os tipos suportados.
- A solução deve suportar automated machine learning based detection engines;
- A solução deve detetar o ataque na fase de *exploitation* - ou seja, antes que o código seja executado e antes que se tenha concluido o download do *malware.*
- A solução deve detetar ROP e outras técnicas de *exploitation* (por exemplo, elevação de privilégios), *analizando* o CPU.
- A solução deve suportar a análise de links no corpo do e-mail para deteção de *Malware Zero Day*.
- A solução deve ser capaz de verificar o histórico de *URLs* registados nos últimos X e-mails e verificar se a classificação foi alterada (por exemplo: de *Clean* para *malicious*).
- Tempo médio de emulação, para um veredito de *malware* suspeito como benigno não deve ser muito superior a 1 minuto.
- Tempo médio de emulação, para um veredito de *malware* suspeito como maligno não deve ser muito superior a 3 minutos.
- A solução de emulação de ameaças deve permitir *Geo Restriction,* que permite que as emulações sejam restritas a um país.
- A solução deve possuir um mecanismo automático de partilha de informação com outros *gateways* em meio a atualizações de assinaturas etc, por forma a partilhar informações sobre novos ataques.
- O mecanismo de emulação deve exceder 90% na taxa de captura nos testes do Total de vírus em que os PDFs e os arquivos maliciosos conhecidos são modificados com cabeçalhos "não usados", para

demonstrar a capacidade das soluções de detetar *malwares* desconhecidos.

- A solução deve detetar o tráfego de C & C de acordo com a reputação dinâmica de IP/URL.
- A solução deve ser capaz de emular e extrair arquivos incorporados em documentos.
- A solução deve ser capaz de analisar documentos com URLs.
- Na funcionalidade de *Sandboxing/Scrubbing,* a solução proposta deverá ter a capacidade de suportar deteção de ameaças e técnicas de evasão (com tentativas de explorar vulnerabilidades de S.O.) ao nível do *CPU – CPU-Level detection*.

b) Deteção de atividades em sistema

- A solução deve ter a capacidade de detetar atividades fora de "padrão de utilização/protocolo":
    - Chamadas de API;
    - Alterações no sistema de arquivos;
    - Alterações de Registo;
    - Ligações de rede;
    - Em Processos do sistema Operativo;
    - Criar e eliminar arquivos;
    - Modificação de arquivos;
    - Adição de código ao *kernel*;
    - Detetar tentativas de elevação de privilégios;
    - Alterações no *kernel* (Alterações de memória realizadas pelo código do *kernel,* não o fato de que um driver ser carregado - isso é controlado pelo item acima);
    - Análise de comportamento do *kernel* (analisar a atividade do código, não as alterações efetuadas pelo utilizador);
    - Contornar UAC (*user access control*).

c) Mecanismos Anti-evasão

- A solução proposta deverá ter capacidade de deteção de técnicas de evasão (emulação/*sandboxing*) para posterior reação e mitigação de ameaças.
- A solução deverá ser resiliente e identificar casos onde a execução de código malicioso (*malware/shell-code*) não ocorra mediante a deteção de

um ambiente virtualizado (técnica de evasão para contornar mecanismos de deteção por *sandboxing*).

- A solução deverá ser resiliente e detetar *delays* implementados na execução de código malicioso (*malware/shell-code*).
- A solução deverá ser resiliente a situações em que a execução de código malicioso (*malware/shell-code*) apenas ocorre após um *restart/shutdown* da *workstation/end point* infetado.

d) Extração de ameaças (*File Scrubbing/Flattening*)

- A solução deverá ter a capacidade de eliminar ameaças existentes em conteúdos dinâmicos/objetos embebidos em ficheiros.
- A solução de proposta deverá ter a capacidade de reconstrução dos ficheiros, excluindo os conteúdos ativos, e mantendo apenas conteúdos seguros.
- A solução deverá ter a capacidade de converter ficheiros reconstruídos (em que os conteúdos ativos foram excluídos) em formato PDF, para serem entregues em tempo real ao utilizador, de forma a melhorar a experiência de utilização.
- A solução proposta deverá ser configurável e flexível, de forma a possibilitar manter o formato do ficheiro original, especificando o tipo de conteúdo a ser removido.

ANEXO II

Mapa de Quantidades

TIPOLOGIA	**QT**
LOTE 1	
EQUIPAMENTOS DE CORE/EDGE	1
TERMINADORES ÓTICOS - SFP 10G BASE SR	8
TERMINADORES ÓTICOS - SFP 10G BASE LR	8
TERMINADORES ÓTICOS - QSFP – 40/100GB -SRBD	4
REQUISITOS GERAIS	v.g.
SERVIÇOS DE IMPLEMENTAÇÃO	v.g.
SUPORTE, MANUTENÇÃO E APOIO TÉCNICO NO LOCAL	v.g.
LOTE 2	
NEXT GENERATION FIREWALL	1
SERVIÇOS DE IMPLEMENTAÇÃO	v.g.
SUPORTE, MANUTENÇÃO E APOIO TÉCNICO NO LOCAL	v.g.

v.g. – Valor Global