



Concurso Público nº 06 - SC/IPS/2022

**Aquisição de Infraestrutura de
Networking Wireless e de Segurança,
para o Instituto Politécnico de Setúbal**

Caderno de Encargos

Concurso Público nº 06 - SC/IPS/2022
Aquisição de Infraestrutura de
Networking Wireless e de Segurança, para o Instituto Politécnico de Setúbal

ÍNDICE

CADERNO DE ENCARGOS	4
1. Objeto do contrato	4
2. Preço base.....	4
3. Exclusão de propostas	4
4. Prazos de execução	4
5. Obrigações de sigilo	5
6. Especificações técnicas	6
7. Preço contratual	6
8. Condições de pagamento	6
9. Cessão da posição contractual	6
10. Subcontratação	6
11. Rescisão do Contrato	7
12. Encargos e Responsabilidade com Patentes	7
13. Cumprimento e Incumprimento.....	7
14. Despesas	9
15. Faturação	9
16. Proteção de Dados.....	9
17. Legislação aplicável	10
ANEXO A	11
1 Requisitos gerais	13
1.1 Gateway de Segurança	13
1.1.1 Integração com redes de comunicações.....	13
1.1.2 Identificação de utilizadores e dispositivos	15
1.1.3 Firewall	16
1.1.4 VPN.....	17
1.1.5 Controlo de aplicações.....	19
1.1.6 Alta disponibilidade	19
1.1.7 Administração, Monitorização e Diagnósticos	20
1.1.8 Registo de eventos e relatórios.....	22
1.1.9 IPS - Detecção e prevenção de intrusões	22
1.1.10 Proteção contra ameaças.....	23
1.1.11 Certificações	26
1.1.12 Especificações do equipamento Setúbal.....	26
1.1.13 Especificações do equipamento Barreiro.....	28
1.2 Solução de Rede Wireless.....	29
1.2.1 Pontos de Acesso Wireless.....	29
1.3 Switches de Acesso	30
1.3.1 Requisitos de Gestão	31
1.3.2 Alta Disponibilidade	31
1.3.3 Requisitos de Segurança	31
1.3.4 Requisitos de Routing.....	32

1.3.5	Requisitos de Layer 2.....	32
1.3.6	Requisitos de Serviços.....	33
1.3.7	Requisitos ao nível do suporte de RFC e MIB.....	33
1.3.8	Conectividade e Sistema:.....	33
1.4	Plataforma de Recolha de Logs.....	34
1.4.1	Relatórios e Ferramentas de Visualização.....	34
1.4.2	APIs JSON e XML (Serviços Web)	35
1.4.3	Visualização de Logs	35
1.4.4	Gestão de Eventos	35
1.4.5	DLP Archiving	36
1.4.6	Especificações técnicas	36
2	Mapa de Quantidades	37
3	Solução para instalações IPS	37
4	Formação e material de apoio	37
5	Suporte de manutenção	38
	Anexo B – Mapa dos Espaços para Instalação da Solução.....	39
	ANEXO C	40
	ANEXO D	41

Concurso Público nº 06 - SC/IPS/2022
Aquisição de Infraestrutura de
Networking Wireless e de Segurança, para o Instituto Politécnico de Setúbal

CADERNO DE ENCARGOS

1. Objeto do contrato

O objeto do contrato consiste, de acordo com as cláusulas técnicas descritas neste caderno de encargos, na aquisição de infraestrutura de Networking Wireless e de segurança, para o Instituto Politécnico de Setúbal (IPS), ao abrigo da alínea a) do n.º 1 do art.º 20 do Código dos Contratos Públicos (CCP).

2. Preço base

O preço base é o preço máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações objeto do contrato que constituem este caderno de encargos, correspondendo ao valor máximo de **272.000,00 euros** (duzentos e setenta e dois mil euros), acrescido de IVA à taxa legal em vigor, não podendo ultrapassar os seguintes valores totais:

- Infraestrutura de Networking Wireless e de segurança – 228.000,00€ (duzentos e vinte e oito mil euros) acrescido de IVA à taxa legal em vigor;
- Suporte de manutenção (prazo máximo dois anos) – 44.000,00€ (quarenta e quatro mil euros) acrescido de IVA à taxa legal em vigor, sendo o valor máximo anual 22.000,00€ (vinte e dois mil euros) acrescido de IVA à taxa legal em vigor.

3. Exclusão de propostas

É excluída a proposta cuja análise revele:

- a) Um preço contratual superior ao preço base;
- b) Características técnicas e funcionais diferentes das especificações exigidas no caderno de encargos.

4. Prazos de execução

- a) O fornecedor terá de garantir a execução de todas as prestações objeto do contrato, com a aceitação definitiva da conclusão do projeto e a

- certificação a toda a ligação à rede existente nos edifícios do IPS, no prazo de entrega máximo de 150 dias, após a assinatura do contrato;
- b) O suporte de manutenção previsto no ponto 5 do Anexo A – Especificações Técnicas, tem a duração de um ano a contar da data da aceitação definitiva da conclusão do projeto com certificação a toda a ligação à rede existente nos edifícios do IPS, e será automaticamente renovado por igual período de um ano se nenhuma das partes o denunciar, mediante notificação à outra por carta registada com aviso de receção, com antecedência mínima de sessenta dias em relação ao seu termo ou à data de renovação;
- c) O prazo máximo de vigência do contrato de manutenção, incluindo renovações, é de dois anos.

5. Obrigações de sigilo

O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra relativa ao IPS, de que possa ter conhecimento, ao abrigo ou em relação com a execução do contrato.

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.

Exclui-se do dever de sigilo previsto a informação e a documentação que forem comprovadamente do domínio público, à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladores ou outras entidades administrativas competentes.

O dever de sigilo mantém-se em vigor até ao termo do prazo de 3 anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

6. Especificações técnicas

A prestação de serviços a fornecer pelo adjudicatário deverá obedecer às especificações técnicas, constantes no caderno de encargos e no Anexo A – Especificações Técnicas.

7. Preço contratual

- a) Pelo fornecimento dos serviços objeto do contrato o IPS pagará o valor total do preço contratual constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor.
- b) Não é admitida a revisão de preços durante o prazo de vigência do contrato.

8. Condições de pagamento

O pagamento será efetuado no prazo de 30 dias seguintes à data da aceitação da fatura, a qual só deve ser emitida, após o vencimento de todas as obrigações a que se refere.

A faturação do suporte de manutenção deve ser emitida mensalmente de acordo com a alínea b) do ponto nº 4 do Caderno de Encargos

Se nada for dito em contrário, a fatura considera-se aceite no prazo de 15 dias úteis a contar da sua receção.

O atraso no pagamento da fatura terá as consequências previstas na lei, designadamente o pagamento dos juros de mora sobre o montante em dívida, nos termos do artigo 326º do CCP.

9. Cessão da posição contractual

A cessão da posição contratual por qualquer das partes depende da autorização da outra, sendo em qualquer caso vedada nas situações previstas no n.º 1 do artigo 317.º do CCP.

10. Subcontratação

O adjudicatário não poderá, por qualquer forma, subcontratar terceiras entidades para a realização de tarefas relativas ao objeto do contrato, sem prévio consentimento do IPS.

11. Rescisão do Contrato

A rescisão não prejudica quaisquer ações de responsabilidade civil por factos verificados durante o período de vigência do contrato.

O incumprimento, por uma das partes, dos deveres resultantes do contrato confere, nos termos gerais do direito, à outra parte o direito de rescindir o contrato, sem prejuízo das correspondentes indemnizações legais.

Para efeitos do disposto no parágrafo anterior, considera-se incumprimento definitivo quando se verificar que o objeto do contrato não corresponde às características e especificações que lhe são atribuídas na proposta e restante documentação apresentada pelo adjudicatário.

12. Encargos e Responsabilidade com Patentes

Serão inteiramente da conta do adjudicatário os encargos e responsabilidades decorrentes da utilização, no fornecimento de materiais, de elementos de construção, de "software" ou "hardware" ou outros que respeitem a quaisquer patentes, licenças, marcas, desenhos registados e outros direitos de propriedade industrial.

Se o IPS vier a ser demandado por ter sido infringido na execução dos trabalhos qualquer dos direitos mencionados no paragrafo anterior, o adjudicatário indemnizá-lo-á integralmente de todas as despesas que haja de fazer, e de todas as quantias que tenha de pagar.

13. Cumprimento e Incumprimento

a. Âmbito

- i. O cumprimento corresponde à realização das prestações a que as partes se encontram vinculadas por efeito do contrato, de forma exata e pontual.
- ii. Nos termos da lei e do contrato, o incumprimento, por facto que lhe seja imputável, constitui o co-contratante no dever de indemnizar o IPS, sem prejuízo da aplicação das sanções contratuais administrativas e da resolução sancionatória, conforme se justifique, ou de outras consequências legalmente previstas.
- iii. As importâncias devidas pelo co-contratante a título indemnizatório ou sancionatório são suscetíveis de compensação nos pagamentos a realizar

pelo IPS, bem como de efetivação através das quantias caucionadas, se existirem.

- iv. As sanções de natureza pecuniária fixadas nas cláusulas seguintes destinam-se a punir o inadimplemento e a compelir o co-contratante a restabelecer o cumprimento das prestações contratuais em falta, não revestindo a natureza de cláusula penal e não obstante a que o IPS seja indemnizado pelo dano excedente.

b. Sanções contratuais de natureza pecuniária

- i. Em caso de incumprimento, em geral, de qualquer obrigação decorrente da lei ou do contrato, o IPS pode aplicar ao cocontratante uma sanção pecuniária em valor correspondente até um por mil do preço contratual, por cada falta e por cada dia em que se mantenha a situação de incumprimento, após notificação para a respetiva supressão.
- ii. O IPS pode ainda aplicar ao co-contratante a sanção prevista no número anterior por cada dia de atraso que lhe seja imputável no cumprimento de qualquer prestação objeto do contrato, sempre que inexistir prazo fixado para o cumprimento da obrigação e este seja fixado pelo IPS, com razoabilidade e por razão justificada, com a antecedência mínima de cinco dias úteis.
- iii. A medida das sanções é determinada em função da gravidade do incumprimento, nomeadamente, considerando a duração da infração, a sua eventual reiteração, o grau de culpa do co-contratante e as consequências que advenham do incumprimento.
- iv. Sem prejuízo do disposto no nº 3 do artigo 329º do CCP, o valor acumulado das sanções pecuniárias aplicadas não pode exceder 20% do preço contratual.

c. Outras sanções contratuais administrativas

- i. Sem prejuízo do direito à resolução e das demais consequências indemnizatórias e sancionatórias, bem como da faculdade estabelecida no artigo 318º-A do CCP, o incumprimento do contrato legitima, subsidiariamente, o IPS a adquirir no mercado as prestações em falta,

suportando o co-contratante quaisquer custos acrescidos que decorram desse facto, incluindo os relacionados com o eventual acréscimo de preço.

14. Despesas

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

15. Faturação

As faturas deverão ser emitidas em nome do Instituto Politécnico de Setúbal, Edifício Sede, *Campus* do IPS – Estefanilha, 2910 - 761 Setúbal, NIPC 503 720 364, **indicando, ainda, o número de compromisso que irá constar na requisição oficial e contrato.**

16. Proteção de Dados

- a) O Instituto Politécnico de Setúbal informa que os eventuais dados pessoais recolhidos no âmbito da celebração e vigência do presente contrato têm por objetivo /finalidade o cumprimento das obrigações decorrentes do mesmo.
- b) Nesta conformidade, os dados necessários podem ser comunicados à Autoridade Tributária e Aduaneira e a quaisquer outras entidades que, de acordo com a lei e os fins que prossigam, tenham direito a aceder aos dados pessoais eventualmente tratados.
- c) Os dados pessoais recolhidos serão guardados e tratados durante o período de vigência do contrato e, após a sua cessação, pelo prazo que a legislação fiscal indicar e que, atualmente, é de dez anos.
- d) O titular dos dados tem o direito de acesso aos seus dados e de requerer a sua retificação, o direito de aceder ao registo do seu tratamento, ao seu apagamento após o decurso dos prazos legais decorrentes da legislação fiscal ou outra aplicável, bem como à sua portabilidade.
- e) Com a adesão ao caderno de encargos o adjudicatário compromete-se expressamente a respeitar o Regulamento Geral de Proteção de Dados, na versão atualmente em vigor e a indicar as respetivas políticas de privacidade que prossegue, que serão anexadas ao contrato.
- f) Com a assinatura do contrato o adjudicatário, compromete-se a assinar a declaração, conforme anexo D, do caderno de encargos.

17. Legislação aplicável

Em tudo o que for omissa no presente caderno de encargos, observar-se-á o disposto no CCP e demais legislação aplicável e, em qualquer caso, sempre a Lei Portuguesa.

ANEXO A

Especificações Técnicas

Introdução

O **Instituto Politécnico de Setúbal (IPS)** pretende adquirir uma nova infraestrutura de *Networking Wireless* e de segurança.

Neste sentido pretende-se que as propostas apresentadas pelos concorrentes incluam as seguintes componentes:

- Gateways de Segurança;
- Pontos de Acesso Wireless;
- Switches de Acesso para a solução Wireless;
- Plataforma de recolha de logs;

Atualmente, o IPS possui 3 sites, interligados por fibra escura, em *Layer 2*, sendo roteamento (*Layer 3*) realizado na totalidade no campus de Setúbal. O diagrama seguinte pretende representar as ligações entre sites.

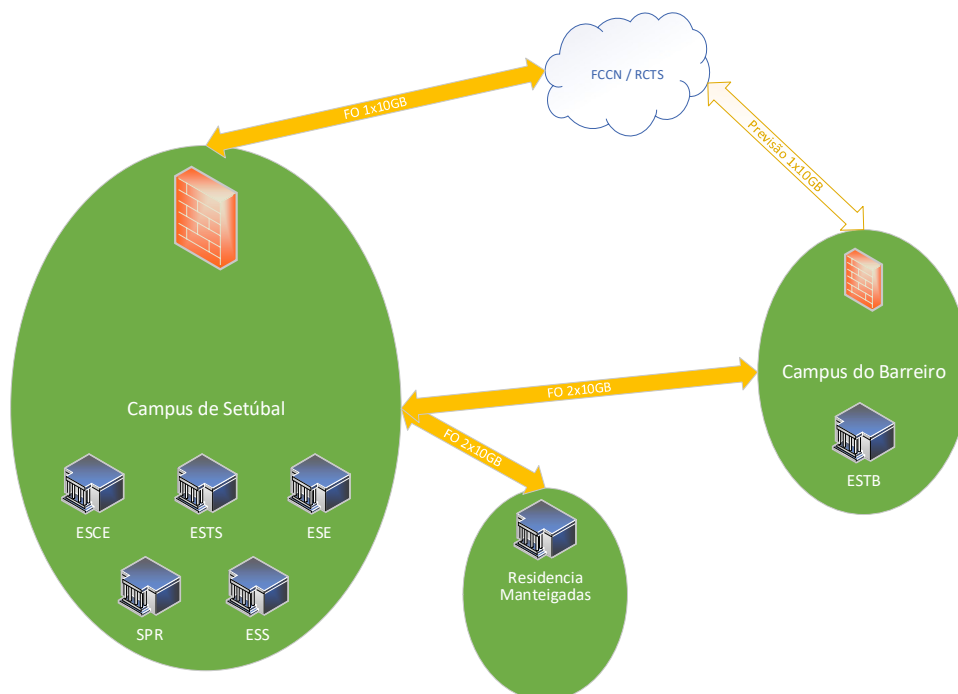


Figura 0.1 – Diagrama Interligações sites IPS.

Neste processo de aquisição pretende-se substituir a solução de segurança existente no IPS, apostando numa solução com redundância em ambos os sites, Setúbal e Barreiro. No campus do Barreiro pretende-se implementar com uma solução de *failover* da solução primária implementada em Setúbal dado que há a possibilidade implementação de uma ligação WAN (seja em ativo/ativo ou ativo/passivo).

Pretende-se que a solução de gateway ofereça uma solução de acesso remoto por VPN (em redundância nos sites).

Adicionalmente, pretende-se adquirir a implementação de uma solução *Wifi* composta pelos pontos de acesso, cujo número será determinado mediante *site survey*, equipamentos de *switching* de acesso dedicados à solução, respetiva controladora e todos os componentes necessários para o correto funcionamento (ex: passagem de cabos, aparelhagens, etc).

Complementando as soluções, pretende-se que seja implementada uma plataforma de recolha de *logs* dos sistemas adquiridos.

1 Requisitos gerais

Com o objetivo de simplificar a gestão da infraestrutura, permitindo uma maior flexibilidade e gestão de recursos, a solução a apresentar deverá ser integralmente da mesma marca/fabricante, possibilitando desta forma que exista uma maior integração e correlação das soluções a implementar.

Os requisitos apresentados neste ponto 1. têm carácter obrigatório, à exceção dos identificados como “valorizado”, que são facultativos mas majorados no mérito de qualidade da proposta.

A solução a apresentar deverá prever o suporte de manutenção e subscrição de todos os serviços de segurança, por parte do fabricante, por um período de 2 anos.

1.1 Gateway de Segurança

Pretende-se a implementação de um cluster de *firewalls* para o perímetro da rede, em cada um dos sites (Setúbal e Barreiro) a ser composto por dois equipamentos de forma a garantir redundância e alta disponibilidade, devendo cada um dos equipamentos garantir o conjunto de funcionalidades e especificações técnicas enumeradas de seguida:

1.1.1 Integração com redes de comunicações

As seguintes funcionalidades terão de 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;*
 - *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: *RIPv1, 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 (valorizado);*
- 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*;
- Virtualização da solução em contextos.

- Controlador *Wireless* seja integrado e com capacidade para suportar no mínimo de 2000 pontos de acesso *wireless* (valorizado)
- Controlador *Switching* seja integrado com capacidade para suportar no mínimo de 190 equipamentos de *switching*(valorizado).

1.1.2 Identificação de utilizadores e dispositivos

As seguintes funcionalidades terão de 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*;
 - Cliente VPN;
 - 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)*;
 - Autorrenovação 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 soluções de terceiras partes;
- Identificação de dispositivos:

- 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.

1.1.3 Firewall

As seguintes funcionalidades terão de ser suportadas:

- Modos de operação *NAT/Route* e *Transparent/bridge*;
- Agendamento de políticas: recorrentes ou apenas uma vez;
- 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: predefinidos, 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 *IPv4* e *IPv6* feito em processador.

1.1.4 VPN

As seguintes funcionalidades terão de 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*

- Validação da integridade do dispositivo cliente e do sistema operativo;
- Opção para limpeza de cache aquando da terminação 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.

1.1.5 Controlo de aplicações

As seguintes funcionalidades terão de ser suportadas:

- Deteção de mais de 3000 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;
- Deteção de aplicações mesmo dentro de ligações proxy;
- Diferentes ações de controlo de aplicações: bloquear, *reset* de sessão, monitorização, aplicação de gestão de largura de banda;
- Inspeção SSL (suporte TLS 1.3);

1.1.6 Alta disponibilidade

As seguintes funcionalidades terão de 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 HA*;
 - Suporte para HA com equipamento geograficamente dispersos;
- Opção de sincronização de sessões em equipamentos configurados em modo *Standalone* ou *Cluster geográfico*.

1.1.7 Administração, Monitorização e Diagnósticos

As seguintes funcionalidades terão de ser suportadas:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser;
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica;
- Suporte de linguagens de administração no acesso gráfico, incluindo: português e inglês;
- 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 (IPFIX)*;
- 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 (incluído de terceiras partes) através de scripts CLI e APIs;
- Wizards de configuração para implementação rápida da solução;
- Integração com soluções de Public SDN:
 - Amazon Web Services (AWS);
 - Microsoft Azure;
 - Google Cloud Platform (GCP);
 - Oracle Cloud Infrastructure (OCI);
 - AliCloud;
- Integração com solução de Private SDN:
 - Kubernetes;
 - VMware ESXi;
 - VMware NSX;
 - Openstack (Horizon);
 - Application Centric Infrastructure (ACI);
 - Nuage Virtualized Services Platform e Cisco ACI;
- Funcionalidades de automação para resposta automatizada a eventos, por exemplo: a colocação em quarentena de um dispositivo com um elevado indicador de comprometimento.

1.1.8 Registo de eventos e relatórios

As seguintes funcionalidades terão de ser suportadas:

- Suporte para registo de eventos (*logs*) em diferentes repositórios, tais como: memória, 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;
- Exportação de relatórios(*valorizado*);
- 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 encurtado 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.

1.1.9 IPS - Detecção e prevenção de intrusões

As seguintes funcionalidades terão de ser suportadas:

- Suporte de IPS com deteção de 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: definido por defeito na assinatura, monitorizar, bloquear, reset de sessão ou quarentena (IP do atacante, IP de atacante e vítima, interface de entrada) com definição de duração;
- Registo integral do pacote onde foi detetado o ataque (valorizado);
- 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);
- Implementação de IDS em modo sniffer(valorizado);
- Criação de novas assinaturas (valorizado).

1.1.10 Proteção contra ameaças

As seguintes funcionalidades terão de ser suportadas:

- Inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, *antivírus*, filtragem WEB 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 antivírus, em modo flow, nos seguintes protocolos: *HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP*
- Suporte de antivírus em modo proxy, incluindo:
 - Suporte dos seguintes protocolos: *HTTP/HTTPS, SMTP/SMTPS, 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)
 - Definição manual de filtragem sites com base em URL, conteúdo web e cabeçalho MIME
 - Categorização dinâmica em tempo real, baseada na cloud.
 - 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
 - Registar 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 customizada 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
 - Executar as ações: 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 filtragem disponíveis, tais como tamanho, 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

- Arquivamento 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

1.1.11 Certificações

Os equipamentos terão de ter as seguintes certificações:

- ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN e USGv6/IPv6

1.1.12 Especificações do equipamento Setúbal

1.1.12.1 Conectividade

As seguintes interfaces mínimas terão de ser asseguradas:

- Interfaces 10/100/1000 GE RJ45 Aceleradas por *Hardware*: 16
- Interfaces GE SFP *Slots* Aceleradas por *Hardware*: 8
- Interfaces 25 GE SFP28/10 GE SFP+/GE SFP *Slots* Aceleradas por *Hardware*: 12
- Interfaces 40 GE QSFP+ Aceleradas por *Hardware*: 4
- Interfaces 10 GE SFP+/GE SFP HA *Slots*: 2
- Interfaces de Gestão GE RJ45: 2
- Interface de Consola RJ45: 1
- Interface USB 3.0: 1

1.1.12.2 Desempenho

As seguintes características mínimas terão de ser asseguradas:

- Aceleração do tráfego de Firewall IPv4/IPv6, IPsec VPN, CAPWAP, VXLAN e túneis GRE em hardware dedicado

- Proteção contra ataques de DDoS volumétricos em hardware dedicado
- Aceleração de tráfego NGFW em hardware dedicado
- Débito firewall IPv4 e IPv6 (pacotes UDP de 1518 / 512 / 64 bytes): 198 / 197 / 140 Gbps
- Latência de firewall (pacotes UDP de 64 bytes): 3.22 μ s
- Débito firewall (pacotes por segundo): 210 Mpps
- Sessões TCP concorrentes: 12 Milhões
- Novas sessões/segundo (TCP): 750.000
- Políticas de firewall: 100.000
- Débito VPN IPsec (pacotes 512 bytes): 55 Gbps
- Túneis IPsec Gateway-to-Gateway: 20.000
- Túneis IPsec cliente remoto: 100.000
- Débito VPN SSL: 11 Gbps
- Débito IPS: 17 Gbps
- Débito de inspeção SSL: 12 Gbps
- Débito de Application Control: 34 Gbps
- Débito NGFW: 11 Gbps
- Débito Threat Protection: 9.1 Gbps
- Domínios Virtuais (por defeito / máximo): 10 / 250
- Máximo de Tokens: 20.000
- Licenciamento ilimitado de utilizadores: SIM
- Fonte de alimentação redundante: SIM
- Dimensões máximas: 2RU

1.1.13 Especificações do equipamento Barreiro

1.1.13.1 Conectividade

As seguintes interfaces mínimas terão de ser asseguradas:

- Interfaces 10G SFP+ Slots: 4
- Interfaces 1GbE SFP Slots: 8
- Interfaces GbE 10/100/1000: 16
- GE RJ45 Management / HA Ports: 1
- Console Port (RJ45): 1

1.1.13.2 Desempenho

As seguintes características mínimas terão de ser asseguradas:

- Aceleração do tráfego de Firewall e IPSec por hardware: Hardware dedicado
- Aceleração de tráfego NGFW por hardware: Hardware dedicado
- Débito firewall IPv4 (pacotes UDP de 1518 / 512 / 64 bytes): 27 / 27 / 11 Gbps
- Latência de firewall (pacotes UDP de 64 bytes): 4.78 µs
- Débito firewall (pacotes por segundo): 16.5 Mpps
- Sessões TCP concorrentes: 3 Milhões
- Novas sessões/segundo (TCP): 280.000
- Políticas de firewall: 10.000
- Débito VPN IPSec (pacotes 512 bytes): 13 Gbps
- Túneis IPsec Gateway-to-Gateway: 2.500
- Túneis IPSec cliente remoto: 16.000
- Débito VPN SSL: 2 Gbps
- Débito IPS: 5 Gbps
- Débito de inspeção SSL: 3.5 Gbps

- Inspeção SSL CPS (IPS, HTTPS diversas cifras): 3.500
- Débito de inspeção SSL para sessões concorrentes: 300.000
- Débito de Application Control: 13 Gbps
- Débito NGFW: 3.5 Gbps
- Débito Threat Protection: 3 Gbps
- Domínios Virtuais (por defeito / máximo): 10 / 10
- Máximo de Tokens: 5.000
- Licenciamento ilimitado de utilizadores: SIM

1.2 Solução de Rede Wireless

Pretende-se realizar a aquisição de uma solução de rede wireless, cujo as quantidades serão determinadas na sequência da visita definida no ponto 8 do Programa de concurso. As necessidades de cobertura estão expostas no Anexo B.

1.2.1 Pontos de Acesso Wireless

- 802.11ax
- Bandas de frequência (GHz): 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
- Capacidades do Rádio 1: 2.4 GHz 20/40 MHz (BPSK, QPSK, QAM64, QAM256, e QAM1024)
- Capacidades do Rádio 2: 5 GHz 4x4 20/40/80 MHz
- SSIDs simultâneos (Mínimo): 16
- Suporte para os seguintes tipos EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST;
- Autenticação de Utilizadores/Dispositivos: WPA, WPA2, e WPA3 com 802.1x ou Preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist;
- Tipos de SSID suportados: Local-Bridge, Tunnel, Mesh
- Especificações IEEE:

- Dataframe: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax (Wi-Fi 6)
- PoE: 802.3af, 802.3at, 802.3az
- VLAN e Link aggregation: 802.1Q, 802.3ad
- Radius: 802.1X
- Roaming e QoS: 802.11e, 802.11k, 802.11r, 802.11v
- Outros: 802.11h, 802.11i, 802.11w;
- Coexistência celular: Sim
- OFDMA
- *Wireless intrusion prevention system*;
- Deverá permitir funcionalidades de análise de espectro;
- O equipamento deverá funcionar em modo *Remote Access Point*;
- O equipamento deverá permitir a descoberta automática de Controladores de Equipamentos Wi-Fi e efetuar o download de configurações para instalações *plug-and-play*;
- O equipamento deverá ter suporte para SNMP;
- O equipamento deverá permitir ser gerido via cloud;
- Gerar relatórios de todos os eventos e performance através de uma plataforma centralizada(valorizado);
- Monitorizar o estado do equipamento a partir de uma plataforma centralizada;
- Certificação *Wi-Fi Alliance*;

1.3 Switches de Acesso

Para a solução pretende-se a aquisição de switches de acesso com funcionalidade PoE, portas em número suficiente e velocidades de transmissão correspondentes aos equipamentos de Wifi propostos (ex: se o AP necessitar de portas multigigabit, o

equipamento terá de suportar essa funcionalidade). Cada uma das unidades deve possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

1.3.1 Requisitos de Gestão

As seguintes funcionalidades terão de ser suportadas:

- Acesso SSH, HTTP/HTTPS, CLI e Web GUI Interface;
- Configuração SNMP v1/v2c/v3;
- O equipamento deverá suportar LLDP (802.1ab, Link Layer Discovery Protocol) (*receive and transmit*);
- *Loop-guard*;
- POE (802.3af, 802.3at, UPOE);
- *Download e Upload Software* via TFTP/FTP/GUI;
- Descoberta automática de múltiplos switches;
- Configuração de VLANs (+4K);
- Recolha de Syslog;
- Permitir configuração e monitorização via HTTP REST APIs;
- Gestão do equipamento através de consola centralizada num ponto único de gestão (valorizado).

1.3.2 Alta Disponibilidade

A seguinte funcionalidade deverá ser suportadas:

- Multi-Chassis Link Aggregation (MC-LAG).

1.3.3 Requisitos de Segurança

As seguintes funcionalidades terão de ser suportadas:

- *802.1x Port Authentication*;
- *TACACS+/RADIUS Admin Access*;

- *Port Mirroring;*
- *Autenticação de administração via RFC 2865 RADIUS;*
- *802.1x autenticação com port-based assignment e mac-based assignment;*
- *802.1x Guest and Fallback VLAN;*
- *802.1x MAC Address Bypass (MAB);*
- *802.1x Dynamic VLAN Assignment;*
- *Syslog, sFlow, SNMP e NetFlow (IPFIX);*
- *ACL Tables;*
- *Suporte QoS: 802.1p;*
- *VLAN tag via ACL;*
- *VLAN tag via MAC/IP/802.1x.*

1.3.4 Requisitos de Routing

As seguintes funcionalidades terão de ser suportadas:

- *Static Routing*
- O equipamento deverá permitir L3 Host/ARP Entries
- Deverá ter capacidade de suportar OSPFv2, RIPv2, VRRP e BGP
- *Static BFD (Bidirectional Forwarding Detection)*

1.3.5 Requisitos de Layer 2

As seguintes funcionalidades terão de ser suportadas:

- *Jumbo Frames;*
- Auto negociação da velocidade dos portos e duplex;
- IEEE 802.1D (*MAC Bridging eSTP*);
- IEEE 802.1w (*Rapid Reconfiguration of Spanning Tree*);
- IEEE 802.1s (*Multiple Spanning Tree Protocol (MSTP)*);
- Edge Port / Port Fast;

- IEEE 802.1Q (VLAN Tagging);
- IEEE 802.3ad (Link Aggregation com LACP);
- O equipamento deverá suportar balanceamento de tráfego *Unicast/Multicast* sobre portos em *trunk* (*dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac*);
- IEEE 802.1AX (Link Aggregation);
- Spanning Tree Instances (com MSTP e CST);
- IEEE 802.3x Flow Control and back-pressure;
- IEEE 802.3; 802.3u,; 802.3z, 1000Base-SX/LX, 802.3ab;
- 802.3 CSMA/CD Access Method and Physical Layer Specifications;
- VLANs baseado por MAC, IP, Ethertype;
- Suporte de Virtual-Wire (valorizado);

1.3.6 Requisitos de Serviços

As seguintes funcionalidades terão de ser suportadas:

- O equipamento deverá suportar IGMP Snooping
- O equipamento deverá suportar deteção e notificações de conflitos de IP;

1.3.7 Requisitos ao nível do suporte de RFC e MIB

As seguintes funcionalidades terão de ser suportadas:

- DHCP relay e DHCP Snooping;
- RFC1157, RFC1213, RFC1354, RFC1573, RFC1643, RFC2030, RFC2571, RFC2572, RFC2865;

1.3.8 Conectividade e Sistema:

As seguintes características mínimas terão de ser asseguradas

- Nº mínimo de interfaces por equipamento:
 - 16 portas a Gbps RJ45 PoE (802.3af/at);
 - 8 portas a multigigabit RJ45 PoE (802.3af/at/bt) (valorizado 802.3bz);

- 4 portas a 10 Gbps SFP+;
- Interface de gestão dedicada 10/100 Mbps: 1
- Interface de Consola RJ45: 1
- PoE Power Budget (mínimo): 420W
- Modo de gestão: Web, CLI e Firewall
- Capacidade de *switching* (Duplex): 172 Gbps
- Pacotes por segundo (Duplex): 250 Mpps
- Armazenamento de *MAC addresses*: 16000
- Baixa latência
- Número de VLANs suportadas: +4000
- Tamanho do grupo *Link Aggregation Group*: até 8
- Capacidade da DRAM (mínimo): 1 GB;
- Capacidade da FLASH (mínimo): 256 MB;
- Fonte de alimentação redundante;
- Altura: 1RU

1.4 Plataforma de Recolha de Logs

Pretende-se a implementação de uma *appliance* virtual para recolha, arquivo e correlação de *logs* e eventos e que garanta o conjunto de especificações e tecnologias enumeradas em seguida:

1.4.1 Relatórios e Ferramentas de Visualização

As seguintes funcionalidades terão de ser suportadas:

- Deteção de anomalias na rede em tempo real;
- Multi-tenant e domínios administrativos de forma a garantir separação de dados e gestão;
- Gestão de utilizadores de administração com base em políticas RBAC;

- Visualização e filtragem ordinária dos utilizadores na utilização das VPNs;
- Visualização dos endereços dos destinos, sites web e ameaças;
- Deverá incluir de base múltiplos modelos de relatórios pré-definidos e prontos a utilizar;
- Relatórios com sumário do tráfego e gestão de ameaças unificadas;
- Capacidade de monitorizar e alertar o administrador de TI sobre eventos importantes;
- Capacidade de importar/exportar modelos de relatórios.

1.4.2 APIs JSON e XML (Serviços Web)

As seguintes funcionalidades terão de ser suportadas:

- Suporte para APIs: JSON e XML.

1.4.3 Visualização de Logs

As seguintes funcionalidades terão de ser suportadas:

- Visualização de *Logs* em tempo real ou por histórico;
- Visualizar por tipo de tráfego ou por *logs* de segurança;
- Visualizar por tipo de dispositivo ou por domínio administrativo;
- Filtragem de *Logs*;
- Visualização de *Logs* de forma granular;
- Apresentação dos *Logs* com pictogramas das aplicações (valorizado);
- *NOC View*;
- *IoC (Indicator of Compromise)*

1.4.4 Gestão de Eventos

As seguintes funcionalidades terão de ser suportadas:

- Criar alertas de forma simples;
- Desencadear alertas consoante o nível de severidade, eventos específicos, por tipo de ações e destinos;

- Definir vários limites pelo número de eventos num determinado período de tempo;
- Visualizar ou procurar alertas através do histórico;
- Notificar por email/SNMP ou enviar eventos por syslog.

1.4.5 DLP Archiving

As seguintes funcionalidades terão de ser suportadas:

- Investigar arquivos DLP;
- Suportar vários tipos de arquivo: *email, HTTP, FTP, IM*.

1.4.6 Especificações técnicas

As seguintes características mínimas terão de ser asseguradas:

- Dispositivos/Contextos suportados (mínimo): 9.900;
- Capacidade de armazenamento mínimo: +3 TB;
- GB/Dia de Logs: +10;
- Virtual CPUs (mínimo/máximo): 4 / Ilimitado;
- Virtual NICs (mínimo/máximo): 1 / 4;
- Suporte de Hypervisor: VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0, Microsoft Hyper-V 2012 R2/2016, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), Alibaba Cloud (AliCloud);

2 Mapa de Quantidades

Em seguida apresentamos uma tabela que resume as necessidades previstas e respetivas quantidades.

Descrição	Quantidade
Gateway de Segurança	4 (2 Campus Setúbal e 2 Campus Barreiro)
Pontos de Acesso Wireless	A determinar após visita (no mínimo, um total de 180 APs)
Switches	A determinar após visita para ligação dos APs (no mínimo, um total de 17 switches)
Plataforma de recolha de logs	1

Tabela 1 – tabela de quantidades desejadas.

3 Solução para instalações IPS

A solução tecnológica preconizada compreende o fornecimento, instalação, configuração, certificação e toda a ligação à rede existente nos edifícios do IPS, incluindo todos os cabos, acessórios, tomadas, calhas técnicas, terminais de ligação e trabalhos de intervenção para atravessamento de divisórias, respeitando as normas e boas práticas na execução dos trabalhos análogos.

Toda a instalação deve ser adaptada às características dos espaços e edifícios, sem que qualquer cablagem esteja visível. Os trabalhos de intervenção para atravessamento de divisórias estão sujeitos a apresentação de plano e aprovação prévia à sua execução.

4 Formação e material de apoio

Na proposta deverá estar incluída a realização de uma formação presencial, após a conclusão da instalação, aos elementos da Divisão Informática, no mínimo 7 horas, para disseminação do funcionamento e gestão de todas soluções implementadas. Deverão ser produzidos materiais de apoio da instalação/configuração/utilização da infraestrutura (equipamentos, configurações, ligações, etc) com recurso a vídeos ou online.

Deverá ser entregue uma lista de todos os equipamentos instalados com os seguintes dados: equipamento, descrição e número de série.

5 Suporte de manutenção

Os serviços a fornecer no período de manutenção (3 anos) deverão corresponder aos seguintes requisitos:

- Assistência telefónica disponível nos dias úteis das 8h às 20h;
- Acesso a plataforma de apoio técnico 24hx365dias;
- Acesso à knowledge base, recursos, comunidades e ferramentas online dos equipamentos, 24hx365d;
- Atualizações de software e firmware;
- Maintenance Releases;
- Reposição de Hardware avariado com deslocação incluída.

Tempo de resposta:

- Crítico: 8 horas;
- Grave: próximo dia útil;
- Normal: 48H.

Anexo B – Mapa dos Espaços para Instalação da Solução

Campus Setúbal		
Edifícios	Sinal	Espaços
ESCE/ESS	Moderado	A1.00,D1.01,D1.02,D1.03,D1.04,D1.09,A2.02,A2.07,C2.19,C2.24,D2.09,D2.10,D2.12,D2.15,D2.16,D2.17,D2.18,D2.19,D2.21,D2.22,D2.23,D2.24,A3.04,A3.07,A3.09,A3.10,A3.11,A3.13,D3.01,D3.12,D3.13,D3.14,D3.15,D3.16,D3.17,D3.18,D3.19,D3.20,D3.21,B1.17E,B1.18,C1.17,D1.10,D2.09,D2.11,D2.13,A3.02,A3.03
	Intensivo	B1.04,B1.05,B1.06,B1.07,B1.08,B1.12,B1.13,B1.15,B1.16,B1.17D,A2.06,A2.12,B2.17,B2.19,B2.21,B2.23,B2.24,B2.28,B2.29,B2.30,B2.31,B2.32,B2.33,B2.34,B2.35,B2.36,B2.37,B2.38,B2.39,B2.40,B2.41,B2.42,B2.43,B2.44,B2.45,B2.46,B2.47,A1.01,A1.02,B1.01,B1.03,C1.04,C1.05,C1.06,C1.07,C1.08,C1.12,C1.13,C1.15,C1.16,C1.18,A2.03,A2.04,A2.08,B2.01,B2.02,B2.03,B2.04,B2.05,B2.06,B2.07,B2.08,B2.09,B2.10,B2.11,B2.12,B2.13,B2.14,B2.15,B2.16,B2.18,B2.20,B2.22,C2.01,C2.02,C2.03,C2.04,C2.05,C2.06,C2.07,C2.08,C2.09,C2.10,C2.11,C2.12,C2.13,C2.14,C2.15,C2.16,C2.17,C2.18,C2.20,C2.25,C2.26,C2.27,C2.28,C2.29,C2.30,C2.31,C2.32,C2.33,C2.3,C2.35,C2.36,C2.37,C2.38,C2.39,C2.40,C2.41,C2.42,C2.43,D2.02,D2.14,D2.20
ESE	Moderado	S12, S13, L4, S14, Sala Reuniões (G1), S1, S2, S3, S4, L1, G5, Ginásio, L2, L7, S6, S7, S8, S9, S10, S11, L3
	Intensivo	G6, Bar, Biblioteca, Audiovisuais 17 e 14, G17,CD2, S15, Galeria, Hall estúdio
ESTS	Moderado	D103, D105, D106, D107, D109, D110, D111, D113, D114, D115, D117, D119, D120, D204, D205, D207, D208, D210, D211, D212, D214, D215, D304, D305, D306, D308, D309, D310, D311A, D311B, D311C, D312, D313, D314, D315A, D315B, D315C, D316, D317, D321, D326, E106, E107, E108, E110, E111, E112, E114, E115, E116, E118, E119, E120, E121, E203,E204, E205, E206, E207, E209, E210,E211, E212, E213A, E365, E364, E362,E361, E360, E358, E357, E356, E355, E3554, E553, E351, E303, E305, E307,E308, E309, E311, E312, E313, E315, E316, E317, E319B, F151, F152, F153, F155, F157, F104, F105, F108, F109, F110, F252, F254, F255, F256, F257, F259, F260, F261, F262, F264, F269, F265, F266, F267, F268, F203, F204B, F207, F208, F209, F210, F211, F212A, F369A, F369B, F366, F362, F356, F351, F352, F353, F354, F355, F357, F358, F364, F365, F303, F305, F306, F307, F309, F310, F311, F313, F314A, F318, A261, A262
	Intensivo	D104, D108, D112, D116, D118, D121, D203, D205, D209, D213, D216, D351,D352, D303, D307, D320A, D318, D319, D322, D325, D324, D323, AE, E103, E104, E109, E113, E117, E122A, E122, E122B, Direção ESTS, Auditórios Piso 2, E202, E208, E2014, E2014A, E363, E359, E352A, E304A, E306, E310, E314, E318, E320B, E321, F103, F106, F107, F107A, F111H, F111B, F258, F253, F252, F212, F370, F368, F367, F304, F308, F312, F315, F316, F317, F318, F319, F320
Serviços da Presidência	Moderado	Restante edifício
	Intensivo	Sala de atos, Sala de reuniões
Campus Barreiro		
Edifícios	Sinal	Espaços
ESTB	Moderado	Todo o edifício
	Intensivo	A052 - A

Sinal Moderado	(>= 1Gbps e >= 60 dispositivos em simultâneo)
Sinal Intensivo	(>= 2 Gbps e >= 150 dispositivos em simultâneo)

ANEXO C

Mapa de Quantidades, Preços a Preencher pelo Concorrente

Mapa enviado em excel

ANEXO D

DECLARAÇÃO DE CONSENTIMENTO

(Regulamento Geral de Proteção de Dados)

(Nome), na qualidade de (indicar) e na sequência da celebração do contrato (especificar) declara ter tomado conhecimento da Política de Proteção de Dados do Instituto Politécnico de Setúbal, dando o seu consentimento para a recolha dos seus dados pessoais.

Mais declara ter conhecimento que os dados recolhidos podem ser comunicados à Autoridade Tributária e Aduaneira e a quaisquer outras entidades que, de acordo com a lei e os fins que prossigam, tenham direito a aceder aos seus dados pessoais.

Setúbal, dia de mês de ano

(Nome)