

CADERNO DE ENCARGOS

175-C-BS-2021 - UPGRADE A

EQUIPAMENTO DE SEGURANÇA

(CIBERSEGURANÇA)

Assinado por : **HERMÍNIO JOSÉ DA CRUZ**

AUGUSTO RODRIGUES

Num. de Identificação: 09276645

Data: 2021.11.10 15:48:17+00'00'



ÍNDICE

CAPÍTULO I - DISPOSIÇÕES GERAIS.....	3
Cláusula 1. ^a - Objeto.....	3
Cláusula 2. ^a - Duração do contrato.....	3
CAPÍTULO II – OBRIGAÇÕES CONTRATUAIS	3
SECÇÃO I - OBRIGAÇÕES DO PRESTADOR DE SERVIÇOS	3
<i>Subsecção I - Disposições gerais</i>	<i>3</i>
Cláusula 3. ^a - Obrigações principais do fornecedor.....	3
Cláusula 4. ^a - Conformidade e operacionalidade dos bens	4
<i>Subsecção II - Dever de sigilo e proteção de dados.....</i>	<i>4</i>
Cláusula 5. ^a - Objeto do dever de sigilo.....	4
Cláusula 6. ^a - Proteção de dados	4
SECÇÃO II - OBRIGAÇÕES DO MUNICÍPIO DE ALCOBÇA	5
Cláusula 7. ^a - Preço contratual.....	5
Cláusula 8. ^a - Preço base.....	5
Cláusula 9. ^a - Condições de pagamento.....	6
CAPÍTULO III - GARANTIA DE CUMPRIMENTO E SEGUROS	6
Cláusula 10. ^a - Garantia de cumprimento contratual	6
Cláusula 11. ^a - Seguros.....	6
CAPÍTULO IV – GESTÃO DO CONTRATO.....	7
Cláusula 12. ^a – Supervisão e controlo	7
Cláusula 13. ^a – Funções do gestor do contrato	7
CAPÍTULO V – CESSÃO DA POSIÇÃO CONTRATUAL.....	8
Cláusula 14. ^a – Cessão e subcontratação da posição contratual por iniciativa do cocontratante.....	8
Cláusula 15. ^a – Cessão da posição contratual por incumprimento do cocontratante.....	8
CAPÍTULO VI – RESOLUÇÃO DO CONTRATO	9
Cláusula 16. ^a - Resolução por parte do Município de Alcobça	9
Cláusula 17. ^a - Resolução por parte do adjudicatário	10
Cláusula 18. ^a – Extinção do Contrato	10
CAPÍTULO VII - DISPOSIÇÕES FINAIS	10
Cláusula 19. ^a - Comunicações e notificações	10
Cláusula 20. ^a - Legislação aplicável	11
ANEXO A - CLÁUSULAS TÉCNICAS	12
Cláusula 1. ^a – Objeto e Condições Gerais	12
Cláusula 2. ^a – Especificações técnicas.....	13

CADERNO DE ENCARGOS - 175-C-BS-2021 - UPGRADE A EQUIPAMENTO DE SEGURANÇA (CIBERSEGURANÇA)

Capítulo I - Disposições gerais

Cláusula 1.^a - Objeto

O presente concurso tem por objeto principal a **Aquisição de upgrade a equipamento e software de segurança (Cibersegurança)**, de acordo com as condições definidas neste Caderno de Encargos.

Cláusula 2.^a – Duração do contrato

A execução do upgrade da solução integral deve ser realizada no prazo máximo de 20 dias após adjudicação, com licenciamento e suporte válido para o período de três anos.

Capítulo II – Obrigações contratuais

Secção I - Obrigações do prestador de serviços

Subsecção I - Disposições gerais

Cláusula 3.^a - Obrigações principais do fornecedor

1 - Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos, decorrem para o fornecedor as seguintes obrigações principais:

- a) Obrigação de entrega dos bens conforme condições apresentadas na sua proposta; e
- b) Obrigação de garantia de qualidade dos bens.

2 — A título acessório, o adjudicatário fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação do serviço, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 4.^a - Conformidade e operacionalidade dos bens

- 1 — O fornecedor obriga-se a entregar ao Município de Alcobça os bens objeto do contrato com as características, especificações e requisitos técnicos previstos no anexo A ao presente Caderno de Encargos, que dele faz parte integrante.
- 2 — Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam.
- 3 — É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.
- 4 — O fornecedor é responsável perante *Município de Alcobça* por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Subsecção II - Dever de sigilo e proteção de dados

Cláusula 5.^a - Objeto do dever de sigilo

- 1 — O fornecedor deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao Município de Alcobça, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
- 2 — A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
- 3 — Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 6.^a – Proteção de dados

- 1 — O artigo 6.º do **Regulamento Geral sobre a Proteção de Dados** indica as situações em que o tratamento de dados é lícito, designadamente quando “*o tratamento for necessário*

para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré – contratuais a pedido do titular de dados”, e “o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito”.

2 — Sempre que sejam remetidos dados pessoais, nomeadamente em relação à equipa de trabalho proposta, os mesmos devem ser acompanhados de declaração de consentimento para o tratamento dos dados para esta finalidade, por parte dos seus titulares.

3 – Nos termos da alínea v) do n.º 1 do artigo 4.º da Portaria n.º 57/2018, de 26 de fevereiro, a **publicitação do contrato**, é feita no Portal BASE, incluindo anexos e aditamentos, **com exceção** das informações que se relacionem com segredos de natureza comercial, industrial ou outra e das **informações respeitantes a dados pessoais**.

Secção II - Obrigações do Município de Alcobça

Cláusula 7.ª - Preço contratual

1 — Pela execução do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, o Município de Alcobça deve pagar ao fornecedor o preço de acordo com as condições adjudicadas, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

2 - O preço contratual apresentado pelo concorrente contém todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao Município de Alcobça, incluindo despesas de alojamento, alimentação e deslocação dos seus meios humanos se necessário, bem como todas as despesas de aquisição, transporte, armazenamento e manutenção dos seus meios materiais.

3 – Durante o contrato não haverá lugar a revisão de preços.

Cláusula 8.ª – Preço base

1 - O preço base global para o contrato definido nos termos da alínea a) do n.º 1 do artigo 47.º do CCP é de € 60.000,00+ IVA.

2 - Nos termos da alínea d) do n.º 2 do artigo 70.º do CCP são excluídas as propostas que apresentem preço contratual superior ao preço base.

Cláusula 9.^a - Condições de pagamento

- 1 - A(s) quantia(s) devidas pelo Município de Alcobaça, nos termos da cláusula anterior, deve(m) ser paga(s) no prazo de 30 dias após a receção pelo Município de Alcobaça das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva e deve fazer sempre referência ao n.º de compromisso e processo.
- 2 — Para o efeito do número anterior, considera-se vencida a obrigação com a realização do upgrade da solução objeto do contrato.
- 3 — Em caso de discordância, por parte do Município de Alcobaça, quanto aos valores indicados nas faturas, deve este comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
- 4 — Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas através de cheque.

Capítulo III - Garantia de cumprimento e seguros

Cláusula 10.^a - Garantia de cumprimento contratual

- 1 — Não é exigida a prestação de caução.
- 2 — O Município pode proceder à retenção de 10% do valor do pagamento a efetuar, sem necessidade de prévia decisão judicial ou arbitral, para satisfação cumprimento defeituoso, incumprimento definitivo pelo adjudicatário das obrigações contratuais ou legais ou para quaisquer outros efeitos especificamente previstos no contrato ou na lei.

Cláusula 11.^a - Seguros

- 1 — É da responsabilidade do adjudicatário a cobertura, através de contratos de seguro da atividade que exerce.
- 2 — O Município de Alcobaça pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos no número anterior, devendo o adjudicatário fornecê-la no prazo de 1 dia útil.

Capítulo IV – Gestão do contrato

Cláusula 12.^a – Supervisão e controlo

1 — O Município de Alcobça designa como gestor do contrato nos termos do artigo 290.º -A do CCP, o especialista de informática Rui Pedro Veríssimo Santos, e nas suas ausências pelo especialista de informática Vitor Manuel Ferreira Rodrigues, com a função de acompanhar permanentemente a execução do contrato.

2 — O adjudicatário deverá nomear um técnico que o represente em tudo o que concerne ao contrato, o qual servirá de interlocutor entre a entidade adjudicante e o adjudicatário para a resolução e/ou conhecimento de quaisquer assuntos inerentes ao objeto do contrato.

3 — Para efeitos do cumprimento do exercício das funções de gestão do contrato o adjudicatário deverá disponibilizar os contactos telefónicos e de endereço eletrónico do representante por si nomeado.

4 — O adjudicatário está sujeito à supervisão da execução do contrato, a qual será assegurada pelo gestor de contrato.

5 — Caso se verifiquem situações anómalas com base nos relatórios emitidos pelo gestor de contrato, será o adjudicatário notificado para regularização imediata das mesmas.

Cláusula 13.^a – Funções do gestor do contrato

1 - O gestor do contrato deve:

- a) Acompanhar permanentemente a execução do contrato assegurando a verificação da execução em conformidade com o contratualizado tendo em consideração as cláusulas fixadas no contrato, conjugadas com o caderno de encargos e a proposta do adjudicatário e demais condições legais no âmbito do objeto do contrato;
- b) Acompanhar a execução do contrato com a frequência adequada ao integral desempenho das suas funções e caso detete desvios, defeitos ou outras anomalias na execução do contrato, deve comunicá-los de imediato ao órgão competente, propondo em relatório fundamentado as medidas corretivas que, em cada caso, se revelem adequadas;
- c) Participar ao órgão competente, bem como, quando a lei o preveja, situações que comprometam a segurança, a qualidade, o preço contratado, assim como o cumprimento do prazo previsto; e
- d) Desempenhar as demais funções e poderes delegados de notificação ao adjudicatário no âmbito da execução do contrato, exceto em matéria de modificação e cessação do

contrato, as quais terão de ser aprovadas pelo órgão competente para autorizar a despesa.

2 - Quando se trate de contratos com especiais características de complexidade técnica ou financeira ou de duração superior a três anos, e sem prejuízo das funções definidas no ponto anterior, o gestor deve:

- a) Recorrer a técnicos em número e qualificações suficientes de forma a que a gestão do contrato abranja todas as áreas contratualizadas; e
- b) Elaborar indicadores de execução quantitativos e qualitativos adequados a cada tipo de contrato, que permitam, entre outros aspetos, medir os níveis de desempenho do cocontratante, a execução financeira, técnica e material do contrato.

Capítulo V – Cessão da posição contratual

Cláusula 14.^a – Cessão e subcontratação da posição contratual por iniciativa do cocontratante

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

2 - A cessão da posição contratual com iniciativa por parte do cocontratante depende da prévia apresentação dos documentos de habilitação, relativos ao potencial cessionário, que foram exigidos ao cedente na fase de formação do contrato.

3 - A autorização da subcontratação depende da prévia apresentação dos documentos de habilitação relativos ao potencial subcontratado, que foram exigidos, ao subcontratante, na fase de formação do contrato.

Cláusula 15.^a – Cessão da posição contratual por incumprimento do cocontratante

1 - Em caso de incumprimento, pelo cocontratante, das suas obrigações, que reúna os pressupostos para a resolução do contrato, o adjudicatário cede a sua posição contratual ao concorrente do procedimento pré -contratual na sequência do qual foi celebrado o presente contrato, que venha a ser indicado pelo contraente público, pela ordem sequencial no referido procedimento.

2 - Para o efeito previsto na parte final do número anterior, o contraente público interpela, gradual e sequencialmente, os concorrentes que participaram no procedimento pré -

contratual original, de acordo com a respetiva classificação final, a fim de concluir um novo contrato para a adjudicação da conclusão dos trabalhos.

3 — A execução do contrato ocorre nas mesmas condições já propostas pelo cedente no procedimento pré -contratual original.

4 — A cessão da posição contratual opera por mero efeito de ato do contraente público, sendo eficaz a partir da data por este indicada.

5 — Os direitos e obrigações do cocontratante, desde que constituídos em data anterior à da notificação do ato referido no número anterior, transmitem -se automaticamente para o cessionário na data de produção de efeitos daquele ato, sem que este a tal se possa opor.

6 — As obrigações assumidas pelo cocontratante depois da notificação referida no n.º 4 apenas vinculam a entidade cessionária quando este assim o declare, após a cessão.

7 — Quando há lugar a caução e a garantias prestadas pelo cocontratante inicial, estas são objeto de redução na proporção do valor das prestações efetivamente executadas e são liberadas seis meses após a data da cessão, ou, no caso de existirem obrigações de garantia, após o final dos respetivos prazos, mediante comunicação dirigida pelo contraente público aos respetivos depositários ou emitentes.

8 — A posição contratual do cocontratante nos subcontratos por si celebrados transmite -se automaticamente para a entidade cessionária, salvo em caso de recusa por parte desta.

Capítulo VI – Resolução do contrato

Cláusula 16.^a - Resolução por parte do Município de Alcobça

1 — Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, o Município de Alcobça pode resolver o contrato, a título sancionatório, no caso de o fornecedor violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente nos seguintes casos:

- a) Atraso, total ou parcial, na entrega dos bens objeto do contrato superior a cinco dias ou declaração escrita do fornecedor de que o atraso em determinada entrega excederá esse prazo;
- b) Fornecimento de bens com características técnicas diferentes.

2 — O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao fornecedor.

Cláusula 17.^a - Resolução por parte do adjudicatário

- 1 — Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, o adjudicatário pode resolver o contrato quando qualquer montante que lhe seja devido esteja em dívida há mais de seis meses ou o montante em dívida exceda 25% do preço contratual, excluindo juros
- 2 — O direito de resolução é exercido por via judicial.
- 3 — Nos casos previstos no n.º 1, o direito de resolução pode ser exercido mediante declaração enviada ao Município de Alcobça, que produz efeitos 30 dias após a receção dessa declaração, salvo se o este último cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.
- 4 — A resolução do contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pelo adjudicatário, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do Código dos Contratos Públicos.

Cláusula 18.^a – Extinção do Contrato

- 1 - O direito de extinguir o contrato poderá ser exercido pela entidade adjudicante e pela entidade adjudicatária, nos termos previstos na Parte III do CCP.
- 2 - Para efeitos do disposto no número anterior, considera-se incumprimento definitivo, quando houver atraso no fornecimento, por um período superior a 15 dias úteis.

Capítulo VII - Disposições finais

Cláusula 19.^a - Comunicações e notificações

- 1 — Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.
- 2 — Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 20.^a - Legislação aplicável

1 - A tudo o que não esteja especialmente previsto aplica-se o regime previsto no Decreto-Lei n.º 18/2008, de 29 de janeiro (Código dos Contratos Públicos) e demais legislação aplicável.

2 – Em respeito pelo n.º 2 do artigo 1.º A do CCP, o adjudicatário compromete-se a executar o contrato em respeito pelas normas aplicáveis em vigor em matéria social, laboral, ambiental, de igualdade de género e de prevenção e combate à corrupção, decorrentes do direito internacional, europeu, nacional ou regional.

ANEXO A - Cláusulas Técnicas

Cláusula 1.^a – Objeto e Condições Gerais

1 – O Município de Alcobça pretende uma solução que vise dar resposta ao seguinte:

- Aquisição de Upgrade da Firewall Fortinet ou equivalente, para a versão mais recente e suportada por FortiOS;
- Aquisição de Fortimail Security ou equivalente;
- Aquisição de Antivírus Forticlient EPP/APT ou equivalente;
- Bolsa de Horas para apoio à exploração e gestão da solução;
- Serviços técnicos especializados.

2 – A solução a apresentar deverá aumentar os níveis de produtividade dos recursos necessários na administração dos sistemas.

3 – Os tempos de resposta deverão ser os seguintes:

- 2,5 dias para efetuar o upgrade da firewall da FortiNet existente, para a mais recente versão, estável e suportada (FortiOS);
- Apoio à exploração e gestão da Solução, sob a forma de bolsa de 20 horas.

4 – A solução global proposta deve prever o licenciamento e suporte válido pelo período de 3 anos.

5 – Os equipamentos e bens propostos na solução têm de ser novos e compatíveis de modo a permitir que a solução funcione sem constrangimentos.

6 – Mapa de quantidades:

Designação	Unidade	Quantidade
Upgrade Firewall 200D para 201F	un.	2
Serviços de Upgrade de Firewall	vg.	1
Fortimail Security	vg.	1
Antivírus Forticlient	un.	350
Bolsa de 20 horas para apoio à exploração e gestão da solução	h	20
Serviços de Migração, testes e formação para a solução proposta	vg.	1

Cláusula 2.^a – Especificações técnicas

1 – TRADEUP DAS FIREWALLS 200D EXISTENTES PARA 2 (DUAS) FIREWALL'S DA FORTIGATE 201F, OU EQUIVALENTE, COM AS SEGUINTE CARACTERÍSTICAS MÍNIMAS:

- Interfaces 10/100/1000 RJ45 Aceleradas ASIC: 16x GE RJ45
- Interfaces GbE SFP ou 10/100/1000 Aceleradas ASIC: 8x GE SFP
- Interfaces 10GbE SFP+ Aceleradas ASIC: 4x 10GE SFP+
- Interfaces de Gestão: 1x GE RJ45
- Interfaces de HÁ: 1x GE RJ45
- Interface USB Client: 1
- Interface de Console (RJ45): 1
- Disco interno: 1x 480 GB SSD
- Aceleração do tráfego de Firewall, SSL e IPSec por hardware: Hardware dedicado
- Aceleração de tráfego NGFW por hardware: Hardware dedicado
- Débito firewall (pacotes UDP de 1518 / 512 / 64 bytes): 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): 280000
- Políticas de firewall: 10000
- 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
- VPN SSL - Máximo recomendado de utilizadores simultâneos: 500
- Débito IPS: 5 Gbps
- Débito de inspeção SSL: 4 Gbps
- 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 FortiAPs controlados (Total / Tunnel Mode): 256 / 128
- Máximo de FortiSwitch controlados: 64
- Máximo de FortiTokens: 5000
- Máximo de FortiClients registados: 600
- Licenciamento ilimitado de utilizadores: SIM
- Alimentação AC: 100–240V AC, 50–60 Hz
- Consumo de energia médio: 104.52 W
- Consumo de energia máximo: 121.94 W
- Dissipação Térmica: 436.98 BTU/h
- Fonte de alimentação redundante: incluída
- Temperatura de funcionamento: 0 - 40 °C
- Humidade: 20 a 90% sem condensação
- Compliance: FCC Part 15B, Class A, CEM RCM, CVVI, UL/cUL, CB, BSMI
- Certificações: ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, IPv6
- Dimensões: Altura: 44 (1RU), Largura: 432 mm, Profundidade: 342 mm
- Peso: 4.6 KG

1.1 - Integração com redes de comunicações

As seguintes funcionalidades deverão ser suportadas:

- Servidor de DHCP, NTP e DNS incluído
- Funcionalidade de DNS Proxy
- Múltiplos modos de configuração de interfaces:
 - Sniffer
 - Agregação de portas (802.3ad)
 - Loopback
 - VLANs (802.1Q e trunk)
 - Software switch
- Routing estáticos e baseado em políticas (PBR - Policy Based Routing)
- SD-WAN
 - Application Awareness & Steering (3000+ Applications Supported)
 - Dynamic WAN Path Controller
 - NGFW with SSL Inspection
 - Dynamic failover times
 - Secure VPN Overlays
 - Single Management Console for Security & SD-WAN
 - Zero-touch provisioning
- Balanceamento e redundância de múltiplos links;
- Suporte para protocolos de routing dinâmico: 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
- Suporte de IPv6
 - Gestão por IPv6
 - Protocolos de routing dinâmico com suporte para IPv6
 - Tunneling de IPv6
 - Processamento firewall e UTM de IPv6
 - NAT64
 - NAT46
 - VPN IPSec IPv6
- Suporte Dual Stack IPv4 e IPv6 em simultâneo
- Suporte VXLAN
- Controlador Wireless integrado
- Controlador Switching integrado
- Virtualização da solução em contextos.

1.2 - Identificação de utilizadores e dispositivos

As seguintes funcionalidades deverão ser suportadas

- Base de dados local de utilizadores;
- Autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+
- Sistema de Single Sign-on de utilizadores:
 - Windows AD
 - Kerberos
 - Novell eDirectory

- FortiClient
- Citrix e Terminal Server
- Radius (accounting message)
- Autenticação de utilizadores no acesso (802.1x, portal cativo)
- PKI e certificados:
 - Certificados X.509
 - Suporte SCEP
 - Criação de Certificate Signing Request (CSR)
 - Auto renovação de certificados antes da data de expiração
 - Suporte OCSP
- Autenticação de 2 fatores
 - Servidor integrado de autenticação por tokens físicos, tokens por software e SMS
 - Integração com terceiras partes
- Identificação de dispositivos
 - 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

1.3 - Firewall

As seguintes funcionalidades deverão ser suportadas:

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

1.4 - VPN

As seguintes funcionalidades deverão ser suportadas:

- IPSEC VPN:
 - Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico
 - Mecanismos de autenticação: certificados ou pre-shared key
 - IPSEC Phase 1 mode: aggressive e main (ID protection) mode
 - Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup
 - Suporte de IKEv1, IKEv2 (RFC 4306)
 - Suporte de IKE mode configuration (como servidor ou cliente), DHCP over IPSEC
 - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
 - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
 - Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
 - Suporte XAuth como cliente ou servidor
 - XAuth para clientes dialup: Server type option (PAP, CHAP, Auto), NAT Traversal option
 - Duração configurável da chave de encriptação IKE e da frequência do NAT traversal keepalive
 - Dead peer detection
 - Replay detection
 - Autokey keep-alive na Phase 2 SA
- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente
- Suporte ADVPN
- Suporte de configuração full-mesh VPN One-click
- Opções de configuração de VPNs IPsec: baseado em routing(route-based) ou baseado em políticas (policy-based)
- VPNs SSL
 - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente
 - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
 - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos
 - Gestão de atalhos (bookmarks) pessoais
 - Gestão de utilizadores concorrentes
 - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
 - Suporte de VPN SSL em modo web:
 - Para clientes remotos equipamentos apenas com um browser web
 - Disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix
 - Suporte para VPN SSL em modo túnel:

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

1.5 - IPS - Detecção e prevenção de intrusões

As seguintes funcionalidades deverão ser suportadas:

- Suporte de IPS com mais de 12000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados
- Diferentes ações de IPS: monitorizar, bloquear, apagar sessão ou quarentena do IP de ataque com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS específicas com base em IPs
- Proteção DoS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer
- Possibilidade de criar novas assinaturas

1.6 - Controlo de aplicações

As seguintes funcionalidades deverão ser suportadas:

- Deteção de mais de 3100 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas
- Controlo avançado de aplicações de IM e Facebook
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco, e/ou protocolo)
- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade
- Deteção de aplicações mesmo dentro de ligações proxy

- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização ou aplicação de gestão de largura de banda
- Inspeção SSL (suporte TLS 1.3)

1.7 - Proteção contra ameaças

As seguintes funcionalidades deverão ser suportadas:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, antivírus, web filtering e DLP
- Capacidade de descriptação de sessões SSL com cópia de tráfego descriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Detecção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
- Suporte de antivírus 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, STMP/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)
 - Possibilidade de definição manual de filtros de sites com base em URL, conteúdo web e cabeçalho MIME
 - Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias
 - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
 - Deverá ser possível ter a opção para ativar 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 customizadas e sobreposição de categorização
 - Mecanismos de exceção à utilização de perfis pré-definidos;
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Prevenção e proteção de fugas de informação - DLP
- Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Possibilidade de executar as ações: registar, bloquear, quarentena de utilizador/IP/Interface
- Filtros pré-definidos incluindo cartões de crédito e número de segurança Social
- Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Opções de filtro disponíveis: tipo de ficheiro, watermark, conteúdo e deteção de encriptação
- Utilização de mecanismos de DLP watermarking , com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
- Fingerprinting de ficheiros
- Armazenamento de ficheiros detetados para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB
- Integração nativa com plataformas externas de filtragem de email, sandbox e WAF
- Feeds de ameaças por Domain Name e/ou IP Address

Controlo de Endpoints

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

1.8 - Alta disponibilidade

As seguintes funcionalidades deverão ser suportadas:

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover)
 - Monitorização de portas e links (locais e remotos)
 - Sem perda de sessões
 - Failover em menos de 1 segundo
 - Notificações de eventos de failover
- Diferentes opções de arquitetura

- HA com agregação de links
- Full mesh HA
- Suporte para HA com equipamentos geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

1.9 - Administração, Monitorização e Diagnósticos

As seguintes funcionalidades deverão ser suportadas:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica
- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: português, inglês, espanhol, francês, japonês, chinês simplificado, chinês tradicional e Coreano
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.
- Integração com outras soluções (externas) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções Openstack, VMWare NSX, e Cisco ACI.
- Automação, por exemplo para colocar em Quarentena um dispositivo com um elevado Indicador de Compromisso.

1.10 - Registo de eventos e relatórios

As seguintes funcionalidades deverão ser suportadas:

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

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

1.11 - Certificações

O equipamento deverá ter as seguintes certificações:

- Certificações ICSA de Firewall, SSL VPN, IPSEC VPN, AV e IPS
- FIPS 140-2 Validated (quando a operar em FIPS mode)
- USGv6 IPv6 Certified

2 – SOFTWARE FORTIMAIL ENTERPRISE BUNDLE W/ ANTISPAM OU EQUIVALENTE, COM AS SEGUINTE CARACTERÍSTICAS MÍNIMAS:

- Hypervisors suportados: VMware ESXi 5.0/5.1/5.5/6.0/6.5, Citrix / OpenSource XenServer 5.6 SP2/6.0 or later, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, KVM (qemu 0.12.1 and later), AWS (Amazon Web Services), Microsoft Azure
- vCPUs suportados (Máximo): 2
- vNICs suportados (Máximo): 4
- Armazenamento interno (Mínimo / Máximo): 250 GB / 2 TB
- Memória recomendada (Mínimo / Máximo): 2 GB / 8 GB
- Sem filas, com base em mensagens de 100 KB
- Routing de Email: 67 000
- Antispam: 54 000
- Antispam + Antivírus: 52 000
- Especificações do sistema
- Domínios de Email Protegidos: 100
- Políticas baseadas no destino (Domínio / Sistema) – Entrada ou Saída: 400 / 1500
- Caixas de Correio em modo servidor: 400
- Antispam, Antivírus, Autenticação e Perfis de conteúdo (por domínio / por sistema): 50/200
- Prevenção de perda de dados: Sim
- Quarentena Centralizada: Sim
- Integração de API do Microsoft 365: Opcional

2.1 - Sistema

As seguintes funcionalidades deverão ser suportadas:

- Várias opções de instalação:
 - Modo Transparente, Gateway e Servidor
 - Implementação na Cloud local, pública ou privada
 - Serviço com gestão na Cloud
- Inspeção de inbound e outbound
- Suporte para múltiplos domínios de email com personalização por domínio
 - Suporte para multi-tenant

- Administração multicamada
- Suporte para endereços de IPV4 e IPV6
- Virtual hosting com Pools de endereço de Origem e/ou Destino
- Autenticação SMTP suportada em LDAP, RADIUS, POP3 e IMAP
- Routing de email baseado em LDAP
- Inspeção por utilizador baseado em atributos LDAP
- Políticas baseadas em localização geográfica
- Interface gráfica para Webmail e/ou gestão de Quarentenas
- Gestão de filas de correio
- Suporte para vários idiomas de Webmail e interface de administração em conformidade com o RFC SMTP
- Interface gráfica em HTML5
- Compatibilidade com serviços na Cloud (Microsoft 365, Google Workspace, Amazon AWS e Microsoft Azure)

2.2 - Proteção Antispam

As seguintes funcionalidades deverão ser suportadas:

- Reputação de domínio e de remetente
- Spam e assinaturas em anexo
- Regras heurísticas dinâmicas
- Proteção em tempo real contra campanhas de ataque
- Categorização de URL incluindo spam, malware e phishing, pornografia, domínios registados recentemente
- Greylisting para endereços IPv4, IPv6 e contas de email
- Reputação do remetente local (baseado em IPv4, IPv6 e End Point ID)
- Análise comportamental
- Integração externa de URI de Spam e listas negras em tempo real (SURBL/RBL)
- Detecção de newsletter suspeita
- Análise de imagem e PDF
- Listas seguras e negras a nível global, por domínio e por utilizador
- Suporte para padrões de identidade do remetente nomeadamente:
 - Sender Policy Framework (SPF)
 - Domain Keys Identified Mail (DKIM)
 - Domain-Based Message Authentication (DMARC)
- Perfis de notificação
- Serviços de Quarentena de sistema com self-service para utilizadores

2.3 - Proteção contra ataques direcionados

As seguintes funcionalidades deverão ser suportadas:

- Desativação e reconstrução de conteúdo:
 - Neutralização de documentos Office e PDF (remoção de conteúdos perigosos)
 - Neutralização de conteúdo HTML de email
 - Remoção de hiperligações (URL)
 - Reescrita de URLs
- Business Email Compromise (BEC):
 - Proteção anti-spoof multinível

- Análise de falsificação de identidade - deteção manual e automática de falsificação de identidade
- Deteção de domínios semelhantes (cousin domains)
- URL Click Protect com rescrita de URL e revalidação em momento de acesso
- Integração com plataforma de Browser Isolation para neutralização de ameaças baseadas em vulnerabilidades de browser

2.4 - API de Integração

As seguintes funcionalidades deverão ser suportadas:

- Integração Microsoft 365:
 - Recuperação de ameaça pós-entrega
 - Agendamento de Verificação
 - Verificação em tempo real
 - Verificação de correio interno

2.5 - Deteção de conteúdos

As seguintes funcionalidades deverão ser suportadas:

- Deteção de Antivírus:
 - Verificação de assinatura CPRL
 - Deteção comportamental baseada em heurística
 - Deteção de Greyware
- Proteção contra campanhas de malware
- Deteção de conteúdos ativos (PDF e documentos Office)
- Verificação das ameaças na remoção da quarentena
- Verificação de hash de ficheiros personalizadas
- Deteção de MIME e tipo de ficheiros
- Prevenção contra perda de dados com deteção de impressões digitais e deteção de dados confidenciais
- Descriptação automática de ficheiros, PDF e documentos Office
- Verificação de PDF e análise de imagem
- Serviço dinâmico de conteúdos para adultos

2.6 - Encriptação

As seguintes funcionalidades deverão ser suportadas:

- Serviço dinâmico de conteúdos para adultos
- Encriptação TLS "Server to Server" com controlo granular do cyphersuite a aplicar
- Suporte S / MIME
- Encriptação sem cliente para o desktop do destinatário utilizando Encriptação com base na Identidade (Identity Based Encryption - IBE)
- Plug-in para o Outlook para ativar a encriptação baseada em identidade (IBE)

2.7 - Gestão, Logs e Reporting

As seguintes funcionalidades deverão ser suportadas:

- Modos de gestão básico / avançado
- Contas de administração baseadas em funções por domínio,
- Atividade, alteração de configurações, logs e relatório de incidentes
- Módulo de relatório integrado
- Rastreio detalhado de mensagens
- Possibilidade de ter logging e reporting externo à plataforma
- Quarentena centralizada para implantações em grande escala
- Suporte SNMP com recurso a MIBs (standards e privadas) com traps baseadas em thresholds
- Suporte a armazenamento local ou externo, incluindo dispositivos iSCSI
- Suporte Syslog Externo
- Open REST API para configuração e gestão

2.8 - Alta Disponibilidade

As seguintes funcionalidades deverão ser suportadas:

- Alta disponibilidade (Modo ativo-passivo, Modo ativo-ativo)
- Sincronização de fila de e-mails e quarentena
- Detecção e notificação de falha de dispositivo
- Status do link, failover e suporte de interface redundante

2.9 - Avançadas

As seguintes funcionalidades deverão ser suportadas:

- Arquivo de e-mails baseados em políticas com opções para armazenamento remoto
- Recursos de servidor de e-mail avançado
 - Interface de webmail
 - Acesso IMAP e POP3
 - Funções de calendário
 - "Undo" de mail enviado
- Integração de SAML 2.0 SSO e ADFS para acesso webmail e ao portal das quarentenas

3 – 350 LICENÇAS ANTIVIRUS FORTICLIENT EPP/APT OU EQUIVALENTE, COM AS SEGUINTE CARATERÍSTICAS MÍNIMAS:**3.1 - Aprovisionamento:**

As seguintes funcionalidades deverão ser suportadas:

- Inventário de software instalado nas máquinas cliente;
- Integração com Windows AD;
- Informação do endpoint em tempo real;
- Painel de vulnerabilidades;
- Aprovisionamento e distribuição centralizada de software;
- Atribuição automática de grupos;
- Definições de sandboxing sincronizadas automaticamente;
- Telemetria em tempo real do endpoint;
- Controlo de acesso dinâmico para imposição da conformidade, criando grupos que podem ser utilizados por uma NGFW para controlos de acesso dinâmicos;
- Quarentena do endpoint que se encontre comprometido;
- Resposta automatizada sem intervenção manual;
- Split Tunnel baseado em aplicações
- Filtros Web com pesquisa por palavra chave/ filtros de YouTube
- Zero Trust com túneis encriptados por sessão para acesso controlado e validado a aplicações
- Proteção de endpoints baseada em serviços cloud

3.2 - Controlo remoto:

As seguintes funcionalidades deverão ser suportadas:

- Análise de antivírus por solicitação;
- Análise de vulnerabilidades por solicitação;
- Quarentena do cliente;

3.3 - Telemetria e monitorização:

As seguintes funcionalidades deverão ser suportadas:

- Informação do cliente (versão do cliente, Sistema Operativo, IP, MAC address, perfil assignado, avatar do utilizador);
- Estado do cliente;
- Envio de relatório de estado para plataforma externa;

3.4 - Segurança do cliente e componente VPN:

As seguintes funcionalidades deverão ser suportadas:

- Dispor de uma solução de Antivírus;

- Detecção de ameaças baseada na cloud;
- Dispor de uma solução de Anti-Exploit;
- Detecção em ambiente sintético on-prem;
- Detecção em ambiente sintético na cloud;
- Funcionalidade de filtragem web;
- Funcionalidade de Firewall aplicacional;
- Suportar IPsec VPN;
- Suportar SSL VPN;
- Controlo de equipamentos USB;
- Possibilidade de ligar à VPN antes do login no Windows;
- Sistemas operativos:
 - Windows 7 (32 bits e 64 bits);
 - Windows 8 e 8.1 (32 bits e 64 bits);
 - Windows 10 (32 bits e 64 bits);
 - Windows server 2008 ou mais recente;
 - Mac OS X 11+ 10.15, 10.14;
 - iOS 9.0 ou posterior
 - Android 5.0 ou posterior
 - Ubuntu 16.04 ou mais recente;
 - Red Hat 7.4 ou mais recente;
 - CentOS 7.4 ou mais recente com KDE ou GNOME.

3.5 - Requisitos do sistema:

As seguintes funcionalidades deverão ser suportadas:

- Suporte para instalação em Windows server 2012 R2 ou mais recente;
- Requisitos mínimos de hardware:
 - Processador de 64 bits dualcore (ou 2 Vcpu) com 2.0GHz;
 - 4GB de RAM;
 - 40GB de espaço livre em disco;
 - Placa de rede Gigabit;
- Suporte para gestão de clientes Windows, Mac, Linux, Chromebooks, IOS e Android;
- Possibilidade de instalação standalone ou integrado com uma NGFW por forma a suportar NAC;

4 –SOFTWARE 1 (UMA) FORTIANALYZER OU EQUIVALENTE, COM AS SEGUINTE CARACTERÍSTICAS MÍNIMAS:

Este software deverá permitir analítica e reporting e deverá possuir licenciamento gratuito para logs até 1Gb/dia. Futuramente caso o Município pretenda adquirir mais de 1Gb/dia deverá ser possível efetuar o upgrade.

- Devices/ADOMs/VDOMs Suportados (Máximo): 10.000
- Capacidade de armazenamento: 200 GB
- GB/Dia de Logs: 1 GB

Máquina Virtual

- Suporte de Hypervisor: VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS))
- Suportar vCPU (Mínimo / Máximo): 1 / Unlimited
- Interfaces de rede (Mínimo / Máximo): 1 / 4

4.1 - Relatórios e Ferramentas de Visualização:

As seguintes funcionalidades deverão ser suportadas:

- Visualização e filtragem dos Top Users utilização das VPNs
- Visualização dos endereços dos destinos, sites web e ameaças
- Deverá ter por omissão vários modelos de relatórios tipo
- Relatórios com o sumário do UTM e Tráfego
- Capacidade de monitorizar e alertar o administrador de TI sobre eventos importantes
- Capacidade de Importar/Exportar modelos de relatórios já criados para outro FortiAnalyzer ou outro ADOM

4.2 - APIs JSON e XML (Serviços Web):

As seguintes funcionalidades deverão ser suportadas:

- Suporte para APIs:
 - JSON API - Permite MSSPs e grandes empresas manipularem os relatórios do FortiAnalyzer, charts/datasets e objetos
 - XML API - Permite aos administradores aprovisionarem/configurarem o FortiAnalyzer e gerar relatórios

4.3 - Visualização de Logs:

As seguintes funcionalidades deverão ser suportadas:

- Visualização de Logs em tempo real ou por histórico
- Visualizar pelo tipo de tráfego ou por logs de segurança

- Visualizar pelo tipo de device, ADOM
- Filtragem de Logs
- Visualização de Logs de forma granular
- Apresentação dos Logs com pictogramas das bandeiras do países e aplicações

Gestão de Eventos:

As seguintes funcionalidades deverão 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 por um determinado tempo
- Visualizar ou procurar alertas através do histórico
- Notificar por email/SNMP ou enviar eventos por syslog

DLP Archiving:

As seguintes funcionalidades deverão ser suportadas:

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