

CADERNO DE ENCARGOS

Consulta Prévia

Aquisição Firewall Nova Geração

Outubro 2022

Índice

CLÁUSULAS JURÍDICAS.....	3
Cláusula 1.^a Objeto	3
Cláusula 2.^a Contrato	3
Cláusula 3.^a Fases e forma de execução do contrato	4
Cláusula 4.^a Prazo	4
Cláusula 5.^a Contagem do prazo.....	4
Cláusula 6.^a Preço base.....	4
Cláusula 7.^a Revisão de preços.....	4
Cláusula 7.^a Condições de faturação e pagamento	5
Cláusula 8.^a Obrigações da Entidade Adjudicatária.....	5
Cláusula 9.^a Obrigações do Contraente Público	7
Cláusula 10.^a Conformidade e operacionalidade dos serviços	7
Cláusula 11.^a Garantia técnica.....	7
Cláusula 12.^a Sanções contratuais.....	8
Cláusula 13.^a Casos fortuitos ou de força maior	8
Cláusula 14.^a Vinculação por parte da Entidade Adjudicatária	9
Cláusula 15.^a Resolução do contrato por parte do Contraente Público	9
Cláusula 16.^a Resolução do contrato por parte da Entidade Adjudicatária	10
Cláusula 17.^a Confidencialidade e proteção de dados pessoais	10
Cláusula 18.^a Subcontratação e cessão da posição contratual	11
Cláusula 19.^a Dever de sigilo	12
Cláusula 20.^a Comunicações e notificações.....	12
Cláusula 21.^a Gestor de contrato	12
Cláusula 22.^a Fiscalização	13
Cláusula 23.^a Foro competente	13
Cláusula 24.^a Dúvidas e omissões	13
Cláusula 25.^a Legislação aplicável	13

CLÁUSULAS JURÍDICAS

Cláusula 1.^a | Objeto

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual por ajusto direto, em conformidade com a alínea d) do nº 1 do artigo 20º do Código dos Contratos Públicos, que tem por objeto a “**Aquisição Firewall Nova Geração**”, como *appliance* a ser instalada no Data Center do Município de Santa Cruz e nos termos descritos na memória descritiva, ambos juntos ao programa do convite e que dele fazem parte integrante;
2. A presente aquisição insere-se na categoria **30230000-0**, descrito como **Equipamento Informático**, constante do Vocabulário Comum para os Contratos Públicos (Common Procurement Vocabulary - CPV) instituído pelo Regulamento (CE) n.º2195/2002, do Parlamento Europeu e do Conselho, de 5 de Novembro de 2002, publicado no Jornal Oficial da União Europeia, n.º L 340, de 16 de Dezembro de 2002, alterado pelo Regulamento (CE) n.º2151/2003, da Comissão, de 16 de Dezembro de 2003, publicado no Jornal Oficial da União Europeia, n.º L 329, de 17 de Dezembro de 2003 (retificada pela Retificação publicada no Jornal Oficial da União Europeia, n.º L 330, de 18 de Dezembro de 2003), e pelo Regulamento (CE) n.º213/2008, da Comissão, de 28 de Novembro de 2007, publicado no Jornal Oficial da União Europeia, n.º L 74, de 15 de Março de 2008.

Cláusula 2.^a | Contrato

1. O contrato é redigido a escrito, em conformidade com o disposto no n.º 1, do artigo 94.º, do Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, e com observância dos procedimentos referidos nos artigos subsequentes do mesmo diploma (artigos 94.º a 106.º).
2. As condições contratuais resultam da conjugação do disposto no convite e no presente Caderno de Encargos com o conteúdo da proposta adjudicada.
3. O contrato a celebrar integra os seguintes elementos:
 - a) O presente Caderno de Encargos;
 - b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c) O suprimimento dos erros e das omissões do Caderno de Encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo Contraente Público para a decisão de contratar;

- d) A proposta adjudicada;
 - e) Os esclarecimentos sobre a proposta adjudicada prestados pela Entidade Adjudicatária.
4. Em caso de divergência entre os documentos referidos no n.º 3 e o clausulado do contrato e os seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º, do Decreto-Lei n.º 18/2008, de 29 de janeiro, e aceites pela Entidade Adjudicatária, nos termos do disposto no artigo 101.º, desse mesmo diploma legal.

Cláusula 3.ª | Fases e forma de execução do contrato

A instalação e respetivos serviços devem ser efetuados em articulação com a **Divisão de Sistemas de Informação do Município de Santa Cruz**, de acordo com memória descritiva presente neste procedimento.

Cláusula 4.ª | Prazo

1. O contrato a celebrar mantém-se em vigor até a cessão de todas as obrigações dele decorrentes.
2. Prazo de fornecimento, não poderá ser superior a **42 (quarenta e dois) dias úteis**, a contar da outorga do contrato.

Cláusula 5.ª | Contagem do prazo

1. Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.

Cláusula 6.ª | Preço base

O preço base global é de EUR 14747,90 (quatorze mil, setecentos quarenta e sete euros e noventa centimos) acrescido de IVA à taxa legal em vigor.

Cláusula 7.ª | Revisão de preços

Em sede do presente contrato, não haverá lugar à revisão de preços salvo se for determinado por ato legislativo ou administrativo.

Cláusula 8.^a | Condições de faturação e pagamento

1. A Entidade Adjudicatária envia ao Município de Santa Cruz, fatura discriminadas referente à aquisição e ao serviço prestado, bem como todos os elementos justificativos do montante a pagar.
2. **A fatura deverá ser emitida em nome do contraente público, com referência aos documentos que lhe deram origem, isto é, deve especificar o número de compromisso, bem como tem de conter a descrição do objeto (bem) a que respeita, as quantidades, os preços unitários e o preço total, sob pena de ser liminarmente devolvida.**
3. O pagamento terá lugar no prazo de 60 (sessenta) dias **após a entrega da respetiva fatura devidamente emitida, designadamente nos termos do número anterior.**
4. Em caso de incumprimento da obrigação estabelecida no número anterior são devidos juros moratórios nos termos da lei.
5. A faturação deverá ser emitida por via eletrónica, nos termos do artigo 299.º B do Código dos Contratos Públicos, exceto nos casos em que ainda não é legalmente obrigatória. A plataforma utilizada para o efeito pelo Município de Santa Cruz é a YET (disponível em <https://yetspace.com/>).
6. Em caso de discordância por parte do contraente público, quanto aos valores indicados na fatura, deve este comunicar ao cocontratante, por escrito, os respetivos fundamentos, ficando o cocontratante obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida ou nota de crédito.
7. Não são admitidos adiantamentos por conta do fornecimento a efetuar.
8. Em caso de devolução de fatura nos termos do número anterior, o prazo de pagamento referido no n.º 3, desta cláusula, será contado a partir da data de receção da fatura, onde conste o número do respetivo número de compromisso.
9. Desde que devidamente emitidas e observado o disposto no n.º 2 as faturas são pagas através de transferência bancária.

Cláusula 9.^a | Obrigações da Entidade Adjudicatária

1. A Entidade Adjudicatária obriga-se a prestar os serviços objeto do contrato ao Contraente Público, com as especificações e requisitos previstos na Parte II, do presente Caderno de Encargos.
2. A Entidade Adjudicatária compromete-se a dar atendimento adequado à satisfação das necessidades do Contraente Público, no que diz respeito à execução dos serviços que se encontram no âmbito desta contratação.

3. Sem prejuízo de outras previstas na Legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais da celebração do contrato, decorrem para a Entidade Adjudicatária, em conformidade com a absoluta subordinação aos princípios da ética profissional, isenção, independência, zelo e competência, as seguintes obrigações:
- a) Prestar os serviços do contrato a celebrar, de acordo com as datas estipuladas pelo Contraente Público e as especificações técnicas, no presente Caderno de Encargos;
 - b) Executar o objeto do contrato de forma profissional e competente, utilizando os conhecimentos técnicos, a diligência, o zelo e a pontualidade, próprios das melhores práticas;
 - c) Recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação dos serviços, bem como ao esclarecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo;
 - d) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que digam respeito ao Município de Santa Cruz obtidas no âmbito da formação e da execução do contrato, nem utilizar para fins alheios àquela execução, abrangendo esta obrigação a todos os seus colaboradores ou terceiros que nele se encontrem envolvidos;
 - e) Comunicar, antecipadamente, ao Município de Santa Cruz os factos que tornem total ou parcialmente impossível a prestação de serviços objeto do presente procedimento ou o cumprimento de qualquer outra das suas obrigações, nos termos do contrato celebrado;
 - f) Não alterar as condições da prestação de serviços fora dos casos previstos no Caderno de Encargos;
 - g) Comunicar ao Município de Santa Cruz a nomeação do/a gestor/a de contrato responsável por todas as comunicações, bem como quaisquer alterações relativamente à sua nomeação;
 - h) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessárias para o pontual cumprimento das obrigações assumidas no contrato;
 - i) Garantir que durante a vigência do contrato não se venha a verificar qualquer dos impedimentos previstos no artigo 55.º, da Lei n.º 18/2008, de 29 de janeiro.
 - j) Dever de possuir seguro de responsabilidade e danos;

4. A Entidade Adjudicatária deve afetar ao objeto do contrato os meios que entender suficientes, de modo a responder às solicitações do Município de Santa Cruz, nos prazos determinados.
5. A título acessório, a Entidade Adjudicatária fica, ainda, obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à integral execução do contrato, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 10.^a | Obrigações do Contraente Público

1. O Contraente Público deve monitorizar o cumprimento contratual, no que concerne às respetivas condições.
2. O Contraente Público deve pagar à Entidade Adjudicatária o preço constante na proposta adjudicada, pela aquisição de serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes no presente Caderno de Encargos.

Cláusula 11.^a | Conformidade e operacionalidade dos serviços

1. Os serviços objeto do contrato devem ser prestados, para os fins a que se destinam, e dotados de todo o material de apoio e documentação necessária à sua utilização.
2. Os serviços objeto do contrato devem ser disponibilizados, faseadamente, consoante os pedidos efetuados pelo Contraente Público.
3. A Entidade Adjudicatária é responsável perante o Município de Santa Cruz por qualquer defeito ou discrepância dos serviços objeto do contrato, que existam no momento em que os mesmos são prestados.
4. A prestação dos serviços deve ser efetuada em tempo útil e durante a vigência do contrato.
5. Todas as despesas e custos com o transporte e meios humanos são da responsabilidade da Entidade Adjudicatária.

Cláusula 12.^a | Garantia técnica

No que se refere à aquisição de serviços pelo Município de Santa Cruz, a Entidade Adjudicatária fica sujeita às exigências legais de conformidade e garantia técnica, bem como demais obrigações de Entidade Adjudicatária, nos prazos aplicáveis aos contratos de aquisição de serviços, nos termos do Código dos Contratos Públicos e demais legislação aplicável.

Cláusula 13.^a | Sanções contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, o Contraente Público pode exigir à Entidade Adjudicatária o pagamento de uma multa de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
 - a) Pelo incumprimento das datas, prazos de prestação de serviços objeto do contrato, e demais prazos estipulados, o Contraente Público pode exigir da Entidade Adjudicatária o pagamento de uma multa, de montante a fixar, em função da gravidade do incumprimento, que poderá oscilar entre 20% e 50% do valor contratual;
 - b) Pela recusa ou atraso na substituição, em devido tempo, dos serviços, não aceites ou imperfeitos, o Município de Santa Cruz, após notificação à Entidade Adjudicatária, poderá, em caso de necessidade, adquirir a outros fornecedores os serviços em falta, ficando a diferença de preço, se houver, a cargo da Entidade Adjudicatária faltosa.
2. As sanções previstas, na presente cláusula, não obstam a que o Contraente Público exija uma indemnização pelo dano excedente.
3. Se a Entidade Adjudicatária não cumprir de forma exata e pontual as obrigações contratuais ou parte delas, por facto que lhe seja imputável, deve o Contraente Público notificá-lo para cumprir dentro de um prazo razoável, salvo, quando o cumprimento, se tenha tornado impossível ou o Contraente Público tenha perdido o interesse na prestação.
4. Em caso de resolução do contrato por incumprimento da Entidade Adjudicatária, o Contraente Público pode exigir-lhe uma sanção de até 20% do valor da proposta apresentada.
5. Na determinação da gravidade do incumprimento, a entidade adjudicante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa da Entidade Adjudicatária e as consequências do incumprimento.

Cláusula 14.^a | Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se por caso fortuito ou de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar, for impedido de cumprir as obrigações assumidas no contrato.

2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
 - a) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo fornecedor de deveres ou ónus que sobre ele recaiam;
 - b) Incêndios ou inundações com origem nas instalações do fornecedor cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - c) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 15.^a | Vinculação por parte da Entidade Adjudicatária

A Entidade Adjudicatária selecionada, para o fornecimento de serviços, obriga-se a aceitar todas as normas do presente Caderno de Encargos.

Cláusula 16.^a | Resolução do contrato por parte do Contraente Público

1. Sem prejuízo de outros fundamentos de resolução do contrato, previstos na Lei, o Contraente Público pode resolver o contrato, a título sancionatório, logo que ocorram quaisquer das seguintes circunstâncias, por razões imputáveis à Entidade Adjudicatária:
 - a) A execução do contrato seja gravemente prejudicada;
 - b) O incumprimento, ainda que parcial, da obrigatoriedade de prestação de serviços;
 - c) A prática de atos dolosos ou negligentes;
 - d) O não cumprimento definitivo das obrigações assumidas em todo o articulado do presente Caderno de Encargos.
2. Para efeitos do disposto no n.º 1, da presente cláusula, considera-se que existe incumprimento definitivo, por parte da Entidade Adjudicatária, quando se verificar

que as prestações em execução do contrato, não correspondem às características e especificações atribuídas na proposta e restante documentação apresentada.

3. O direito de resolução referido, no número anterior, exerce-se mediante declaração enviada à Entidade Adjudicatária.

Cláusula 17.^a | Resolução do contrato por parte da Entidade Adjudicatária

A Entidade Adjudicatária pode resolver o contrato nos casos previstos no artigo 332.º, do Decreto-Lei n.º 18/2008, de 29 de janeiro.

Cláusula 18.^a | Confidencialidade e proteção de dados pessoais

A Entidade Adjudicatária obriga-se, durante a vigência do contrato e mesmo após a sua cessação, a não ceder, revelar, utilizar ou discutir, com quaisquer terceiros, todas e quaisquer informações e/ou elementos que lhe hajam sido confiados pelo Contraente Público ou de que tenha tido conhecimento, no âmbito do contrato ou por causa dele.

1. Os dados pessoais a que a Entidade Adjudicatária tenha acesso ou que lhe sejam transmitidos pelo Contraente Público, ao abrigo do contrato, serão tratados em estrita observância das regras e normas do Contraente Público.
2. A Entidade Adjudicatária compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer outra forma colocar à disposição de terceiros os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pelo Contraente Público ao abrigo do contrato, sem que para tal tenha sido expressamente instruído, por escrito, pelo Contraente Público.
3. No caso em que a Entidade Adjudicatária seja autorizada pelo Contraente Público a subcontratar outras entidades para a aquisição de serviços, o mesmo será o único responsável pela escolha das empresas subcontratadas, bem como por toda a atuação destas.
4. A Entidade Adjudicatária obriga-se a garantir que as empresas, por este subcontratadas, cumprirão o disposto na Lei da Proteção de Dados Pessoais, Lei n.º 58/2019, de 08 de agosto e na demais legislação aplicável, devendo tal obrigação constar nos contratos escritos que a Entidade Adjudicatária celebra com outras entidades por si subcontratadas.
5. A Entidade Adjudicatária obriga-se a cumprir rigorosamente o disposto na Lei da Proteção de Dados Pessoais e demais legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:

- a) Utilizar os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pelo Contraente Público, única e exclusivamente para efeitos da aquisição de serviços objeto deste contrato;
 - b) Observar os termos e condições constantes nos instrumentos de legalização respeitantes aos dados tratados;
 - c) Manter os dados pessoais estritamente confidenciais, cumprindo e garantindo o cumprimento do dever de sigilo profissional relativamente aos mesmos dados pessoais;
 - d) Cumprir quaisquer regras relacionadas com o tratamento de dados pessoais a que o Contraente Público esteja vinculado, desde que tais regras lhe sejam previamente comunicadas;
 - e) Pôr em prática as medidas técnicas e de organização necessárias à proteção de dados pessoais tratados por conta do Contraente Público contra a respetiva destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais;
 - f) Assegurar que os seus colaboradores cumpram todas as obrigações previstas no contrato.
6. A Entidade Adjudicatária será responsável por qualquer prejuízo em que o Contraente Público venha a incorrer em consequência do tratamento, por parte da mesma e/ou dos seus colaboradores, de dados pessoais em violação das normas legais aplicáveis e/ou do disposto no contrato.
7. Para efeitos do disposto, nos números anteriores, da presente cláusula, entende-se por “colaborador” toda e qualquer pessoa singular ou coletiva que preste serviços à Entidade Adjudicatária, incluindo, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido entre a Entidade Adjudicatária e o/a referido/a colaborador/a.
8. A obrigação de sigilo, prevista na presente cláusula, mantém-se mesmo após a cessação do presente contrato, independentemente do motivo por que ocorra.

Cláusula 19.^a | Subcontratação e cessão da posição contratual

A subcontratação pela Entidade Adjudicatária e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do Decreto-Lei n.º 18/2008, de 29 de janeiro.

Cláusula 20.^a | Dever de sigilo

1. A Entidade Adjudicatária deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao Contraente Público de que possa ter conhecimento, no decorrer da 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 nos números anteriores, a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pela Entidade Adjudicatária 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 21.^a | Comunicações e notificações

1. Todas as comunicações a efetuar nos termos deste Caderno de Encargos poderão revestir a forma escrita e serem enviadas por correio eletrónico, visto que segundo o n.º 2, do artigo 26.º, do Decreto-Lei n.º 135/99, de 22 de abril, *a correspondência transmitida por via eletrónica tem o mesmo valor da trocada em suporte de papel, devendo ser-lhe conferida, pela Administração e pelos particulares, idêntico tratamento.*
2. 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.
3. Quaisquer alterações das informações de contacto constantes do contrato devem ser comunicadas à outra parte.

Cláusula 22.^a | Gestor de contrato

1. Em cumprimento do disposto na alínea i), do n.º 1, do artigo 96.º do Decreto-Lei n.º 18/2008, de 29 de janeiro, o Contraente Público designa gestor de contrato, nos termos do artigo 290.º A, **o chefe de divisão, da Divisão de Sistemas de Informação Hugo Miguel Sousa Cró, com o contacto telefónico 291 520 100 e correio eletrónico hugosousa@cm-santacruz.pt** e como seu substituto o técnico de informática **José Nuno Baptista Martins, com o contacto telefónico 291 520 100 e correio eletrónico nuno@cm-santacruz.pt.**

Cláusula 23.^a | Fiscalização

1. Não obstante todos os direitos e deveres decorrentes do presente Caderno de Encargos, a Câmara Municipal de Santa Cruz reveste-se dos poderes conferidos pelo artigo 302.º, da Lei n.º 18/2008, de 29 de janeiro.

Cláusula 24.^a | Foro competente

Para a resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal do Funchal, com expressa renúncia a qualquer outro.

Cláusula 25.^a | Dúvidas e omissões

1. Todas as situações não previstas neste Caderno de Encargos deverão ser alvo de apreciação e deliberação pelo Contraente Público, no uso das suas competências previstas nas alíneas e) e f), do n.º 1, do artigo 23.º, bem como na alínea f), do n.º 1, do artigo 33.º, da Lei n.º 75/2013, de 12 de setembro.
2. Os casos omissos serão igualmente resolvidos por decisão do Contraente Público.

Cláusula 26.^a | Legislação aplicável

1. Em todo o omissos no processo que constitui o presente procedimento, observa-se o disposto no Código dos Contratos Públicos e demais legislação subsidiária.

Memória Descritiva

Aquisição Firewall Nova Geração

Outubro 2022

Especificações técnicas da Solução de Firewall

- A solução a ser proposta deve ter características de Next Generation Firewall e tem de cumprir as seguintes especificações, para comprovar as especificações anexamos um ficheiro de excel ao procedimento onde se deve preencher o cumprimento do requisito e respetivo documento público do fabricante a fazer prova desse requisito.
- O licenciamento do software existente terá a durabilidade de 36 meses.

Especificações técnicas da Solução de Firewall

Hardware (obrigatório dentro do mesmo equipamento):

- Número de portas 1Gbit/s RJ45 ≥ 4
- Número de portas Gigabit SFP+ 10 Gbit/s ≥ 2
- Porta de gestão dedicada "Out of Band"
- Porta de consola RJ45.
- Arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção.
- Deverá estar garantido que a appliance de Firewall quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa.
- Fontes redundantes.

Performance:

- Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) $\geq 6,0$ Gbps.
- Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) $\geq 4,0$ Gbps.
- Performance da appliance com a funcionalidade de VPN IPSec $\geq 4,0$ Gbps
- Número de novas sessões por segundo $\geq 74\ 100$
- Número máximo de sessões $\geq 480\ 000$

Gestão:

- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML.
- Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio.
- Na gestão centralizada deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy.
- Na gestão centralizada deve existir a possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio.
- Possibilidade de editar configurações pendentes que ainda não foram aplicadas.
- Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas.
- Possibilidade de descartar alterações à configuração realizadas.
- Possibilidade de armazenar diferentes versões da configuração.
- Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada.
- Na gestão centralizada deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos.
- Na gestão centralizada deve existir um ponto centralizado para efectuar upgrades e atualizações de versões e assinaturas.
- Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão.
- Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas.
- Na gestão centralizada deve ser possível gerir até 100 firewalls num único servidor de gestão.
- Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds públicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud.
- Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento.

- Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça.
- Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade.

Networking:

- As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3.
- Suporte de IEEE 802.1Q.
- Suporte de IEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo.
- Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP.
- Suporte de routing estático.
- Suporte de DHCP, NAT e PAT.
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas.
- Capacidade de realizar policy based routing através do IP ou rede de origem.
- Capacidade de realizar policy based routing através do utilizador ou grupo.
- Capacidade de realizar policy based routing através do tipo de aplicação.
- Suporte de arquiteturas de alta disponibilidade do tipo activo/passivo e activo/activo.
- Permitir a criação de clusters de alta disponibilidade até 6 membros.
- Suporte para TLS 1.3 e capacidade de descriptar este tráfego.

Identificação de Utilizadores:

- Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP.
- Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory.
- Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores.
- Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores.
- Possibilidade de gerir utilizadores através de API XML.

- Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local.
- Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing.

Funcionalidades Gerais de Segurança:

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança.
- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança.
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino.
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas.
- Capacidade de identificação de subfunções dentro de uma aplicação.
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7
- Possibilidade de agrupar aplicações por categorias de forma a que as políticas de segurança sejam aplicadas por categorias de aplicações.
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP.
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL.
- Capacidade de decifrar tráfego SSH e detectar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling).
- Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego
- Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança.
- Capacidade de forçar o uso de MFA para acesso a determinados recursos. Deve ser possível configurar políticas que forcem qualquer utilizador em determinada

subnet, a utilizar MFA se tentar aceder a um recurso em determinado segmento de rede da organização.

- Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes

IDS/IPS:

- Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças.
- Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas.
- Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos.
- As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma que a aplicação de perfis de proteção se possam realizar com base nestas categorias.
- Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades.
- Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis.
- Deve ser possível converter assinaturas snort e suricata para dentro da plataforma.

Antivirus & Anti-Malware:

- Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C.
- Capacidade de habilitar mecanismos de DNS sinkholing que permitam intercetar pedidos de resolução de nomes para domínios comprometidos com malware.
- Capacidade de definir políticas de antivírus, de forma que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso.
- Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um

destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs).

- Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possam tomar uma ação no caso de um ficheiro malicioso.
- Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações.
- Capacidade de identificar ficheiros não através das suas extensões mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros.
- Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente.
- Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro.
- Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança
- Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados.
- Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing.
- Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detectado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.

URL Filtering:

- Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir

para os permitidos a ação a realizar (permitir, bloquear, permitir mas advertir, etc).

- Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud
- Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação)
- Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web
- A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet
- A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.

DNS Security:

- A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos.
- Este serviço deve utilizar mecanismos de machine learning para detectar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes.
- A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detectar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling).
- A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS.
- Este serviço deve permitir identificar quais as máquinas e utilizadores infectados, sem a necessidade de qualquer alteração na infraestrutura existente.
- A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente.
- Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas.

- Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos.
- Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains.
- A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças.
- A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas.

Sandboxing:

- Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma a que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload).
- Perante uma análise por parte do serviço de Sandboxing na cloud que categoriza a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente).
- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios.
- A tecnologia de Sandboxing tem de ser capaz de inspeccionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP.
- A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.
- Os sistemas de análise de malware devem ser capazes de detectar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux.
- O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o

seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida.

- Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10
- Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS),
- Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)
- Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.
- Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.

Relatórios & Logs:

- A appliance deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais.
- Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas.
- Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf.
- Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detectadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets.
- Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende.
- Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento.
- Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a longo prazo.

- Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema.
- Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detectadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detectados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos.
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível.

Network Packet Broker:

- O equipamento deve ter capacidades de Network Packet Broker de forma a permitir filtrar e encaminhar tráfego para uma cadeia externa de dispositivos de segurança de terceiros para uma análise estendida.
- Capacidade para usar um ou mais dispositivos de segurança de terceiros (Security Chain) como parte do conjunto geral de segurança.
- Capacidade de definir o tráfego encaminhado com base em aplicações, utilizadores, zonas, dispositivos e endereços de IP.
- Capacidade para encaminhar tráfego TLS (Decryption Broker) descriptado e sem ser descriptado.
- Capacidade para assegurar que o caminho para a cadeia de segurança está íntegro e que tenha opções para lidar com o tráfego se a cadeia não estiver operacional.
- Capacidade para suportar tráfego unidirecional e bidirecional na cadeia (Client-to-server e Server-to-client) no mesmo par de interfaces (broker interfaces).
- Capacidade de definir múltiplos perfis e associar o perfil a uma regra/política.
- As regras/políticas devem definir o tráfego a ser encaminhado para a cadeia de segurança e o perfil deve definir como encaminhar esse tráfego, incluindo os interfaces para encaminhamento, monitorização da integridade da cadeia, distribuição de sessão entre várias cadeias e escolha da forma como é encaminhada Routing (Layer 3) ou Transparente Bridge (Layer 1).

Outras Funcionalidades:

- Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade.
- Possibilidade de decifrar tráfego SSL e SSH de forma a que se possa estabelecer políticas de descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados.
- Capacidade de criar exceções à descriptação para determinado tipo de tráfego.
- Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC).
- Possibilidade de enviar tráfego após descriptação para uma interface de port mirror para análise de terceiras partes.
- Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego.
- Capacidade de capturar tráfego em formato pcap exclusivamente quando se detecta um vírus ou um ataque em qualquer um dos motores de proteção.

Mapa de quantidades:

Descrição	Quantidade
Appliance de Segurança	1
Licenciamento com a subscrição 36 meses:	1
Firewall Aplicacional (Layer7)	
Controlo de utilizadores	
Threat Prevention	
IDS/IPS	
Antivirus & Anti-Malware	
AntiSpyware	
URL Filtering	
Sandabox	
DNS Security	
Análise de eventos	
Reporting	

Amber