Universidade do Minho



Universidade do Minho

CONCURSO PÚBLICO

CCP USSIC-21/2022

LICENCIAMENTO DE SOLUÇÃO DE SEGURANÇA ENDPOINT INTEGRADA COM FIREWALL PALOALTO

CADERNO DE ENCARGOS

Conteúdo

Parte I 4
Capítulo I Disposições gerais 4
Cláusula 1.ª Objeto 4
Cláusula 2.ª Partes integrantes do contrato 4
Cláusula 3.ª Prazo de execução do contrato 4
Capítulo II Obrigações contratuais 5
Secção I Obrigações do fornecedor 5
Cláusula 4.ª Obrigações principais do adjudicatário 5
Cláusula 5.ª Encargos com direitos de propriedade intelectual ou industrial 6
Cláusula 6.ª Verificação e aceitação do objeto do contrato 6
Cláusula 7.ª Objeto e prazo do dever de sigilo 6
Cláusula 8.ª Regulamento de Proteção de Dados 7
Secção II Obrigações da entidade adjudicante 7
Cláusula 9.ª Preço base 7
Cláusula 10.ª Preço contratual e condições de pagamento 8
Capítulo III Incumprimento do contrato 8
Cláusula 11.ª Penalidades Contratuais 8
Cláusula 12.ª Gestor do Contrato 9
Cláusula 13.ª Revogação do contrato 9
Cláusula 14.ª Resolução por parte do contraente público 9
Cláusula 15.ª Resolução por parte do adjudicatário 9
Cláusula 16.ª Casos fortuitos ou de força maior 10
Cláusula 17.ª Subcontratação e cessão da posição contratual 10
Cláusula 18.ª Cessão da posição contratual por incumprimento do cocontratante 10
Cláusula 19.ª Comunicações e notificações 10
Cláusula 20.ª Foro Competente 10
Cláusula 21.ª Legislação aplicável 11
Parte II – Cláusulas e Especificações Técnicas 11
Cláusula 22.ª Âmbito 11
Cláusula 23.ª Especificações técnicas 11

Parte I

Capítulo I
Disposições gerais

Cláusula 1.ª
Objeto

1.O presente procedimento tem por objeto principal a aquisição por um ano de solução de segurança endpoint com 200 licenças, para integrar com a solução de firewall Palo Alto que a UMinho tem atualmente em funcionamento como proteção interna dos serviços digitais críticos alojados no datacenter da Uminho, em conformidade com os termos, condições e características constantes da Parte II – Cláusulas e Especificações Técnicas.

2. O objeto do contrato a celebrar abrange aquisição do licenciamento do módulo, sua instalação e configuração nas instalações da Universidade do Minho, em local posteriormente indicado pela entidade adjudicante.

3. O objeto do contrato abrange ainda os serviços de Suporte Técnico no âmbito da garantia

Cláusula 2.ª
Partes integrantes do contrato

1 – O contrato a celebrar será reduzido a escrito, nos termos do artigo 94.º do Código dos Contratos Públicos (CCP), aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, com as atualizações em vigor, sem prejuízo do disposto no artigo 95.º do referido diploma.
2 – Fazem parte integrante do contrato os seguintes documentos, independentemente da sua redução a escrito, os seguintes documentos:

a) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
b) Os esclarecimentos e as retificações relativos ao caderno de encargos;
c) O presente caderno de encargos;
d) A proposta adjudicada;
e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3 – Em caso de divergência entre os documentos referidos no n.º 2, a prevalência é determinada pela ordem pela qual aí são indicados.
4 – Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato, quando este for reduzido a escrito, prevalecem os primeiros, salvo quanto aos ajustamentos ao conteúdo do contrato propostos, de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos e aceites pelo adjudicatário, nos termos do disposto no artigo 101.º deste mesmo diploma legal.

Cláusula 3.ª
Prazo de execução do contrato

1. O contrato mantém-se em vigor desde a sua celebração até ao termo do período de licenciamento contratado, 1 (um) ano, em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

2. As licenças devem ser entregues no prazo máximo de 30 dias (seguidos) contados da data de assinatura do contrato.

3. A entrega das licenças de software referida no número anterior pressupõe a instalação e configuração dos mesmos, em conformidade com o disposto no nº 2 da clausula 1ª do presente caderno de encargos.

Capítulo II
Obrigações contratuais

Secção I
Obrigações do fornecedor

Cláusula 4.ª
Obrigações principais do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente caderno de encargos, nomeadamente nas especificações técnicas ou nas cláusulas contratuais, da celebração do contrato decorrem para o adjudicatário as seguintes obrigações:

a) Fornecimento das licenças de software, sua instalação e configuração em conformidade com as condições, características, requisitos técnicos e funcionais e condições de garantia definidos no presente caderno de encargos e demais documentos contratuais;

b) Ter ao seu serviço pessoal de reconhecida idoneidade moral, aptidão física e adequada formação técnica;

c) Utilizar corretamente as instalações e equipamentos que lhe forem confiadas, não lhes dando uso diferente do que lhes é devido, respeitando as instruções de utilização e/ou funcionamento que lhe sejam dadas pela UMinho, bem como, e em especial as regras de segurança aplicáveis, designadamente no que respeita às chaves das instalações.

d) Comunicar à UMinho a nomeação do Gestor de Cliente responsável pelo contrato celebrado e quaisquer alterações relativas à sua nomeação;

e) Assegurar que para todas as matérias colocadas pela UMinho ao respetivo Gestor de Cliente, o tempo de resposta não exceda 10 (dez) dias úteis, nas situações normais e 3 (três) dia úteis nas situações urgentes;

f) Responsabilizar-se pelos danos causados diretamente à UMinho, ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato;

g) Comunicar, antecipadamente, à UMinho, de forma fundamentada, logo que deles tenha conhecimento, os factos que tornem total ou parcialmente impossível a entrega de licenças de software ou a prestação dos serviços ou o cumprimento de qualquer obrigação, obrigando-se, se tal for aceite e oportuno, a restabelecer a prestação ou reparar o incumprimento em prazo razoável;

h) Manter durante a execução do contrato, todas as condições de habilitação e qualificação exigidas no procedimento de aquisição, bem como a situação tributária e perante a segurança social regularizadas;

i) Comunicar qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação social, os seus representantes legais com relevância para a prestação, a sua situação jurídica ou situação comercial, bem como as alterações aos contratos e moradas indicadas no contrato para a sua gestão;

2.O adjudicatário fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação dos serviços, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das prestações contratuais a que está obrigado.

Cláusula 5.ª
Encargos com direitos de propriedade intelectual ou industrial

São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, no âmbito do contrato celebrado, de direitos de propriedade intelectual ou industrial, nos termos do artigo 447.º do CCP.

Cláusula 6.ª
Verificação e aceitação do objeto do contrato

1 – Sem prejuízo de outras diligências especialmente previstas na parte II, uma vez executados os serviços objeto do contrato e entregues os elementos correspondentes, a Universidade do Minho, por si ou através de terceiro por ela designado, procede no prazo de 20 dias à análise quantitativa e qualitativa do serviços entregues, com vista a verificar, respetivamente, se os mesmos reúnem as características e requisitos técnicos e operacionais definidos na parte II do presente caderno de encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.
2 – Na análise a que se refere o número anterior, o adjudicatário deve prestar à Universidade do Minho toda a cooperação e esclarecimentos necessários.
3 – No caso da análise a que se refere o n.º 1 não comprovar a total conformidade dos elementos entregues e/ou dos serviços prestados com as exigências legais, ou no caso de existirem discrepâncias com os termos e condições definidos no presente caderno de encargos e na proposta adjudicada, a Universidade do Minho informará, por escrito, o adjudicatário.
4 – No caso previsto no número anterior, o adjudicatário deve proceder, à sua custa, no prazo razoável que for determinado pela Universidade do Minho, aos ajustamentos e/ou complementos necessários para garantir a conformidade dos bens e o integral cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
5 – Após a realização dos ajustamentos e/ou complementos necessários pelo adjudicatário, no prazo respetivo, a Universidade do Minho procede a nova análise, nos termos do n.º 1.
6 – Caso a análise a que se refere o n.º 1 comprove a total conformidade dos serviços prestados com as exigências legais, e neles não sejam detetadas quaisquer discrepâncias com os termos e condições definidos no presente caderno de encargos e na proposta adjudicada, será emitida no prazo máximo de 10 dias, a contar do termo dessa análise, uma **Declaração de Aceitação,** pelo Universidade do Minho.
7 – A emissão da declaração a que se refere o número anterior não implica a aceitação de eventuais discrepâncias com as exigências legais ou com as caraterísticas, especificações e requisitos técnicos previstos no presente caderno de encargos e na proposta adjudicada, que não eram visíveis e/ou não podiam ser detetados

Cláusula 7.ª
Objeto e prazo do dever de sigilo

1 – O adjudicatário deve guardar sigilo e garantir a confidencialidade, não divulgando as condições estabelecidas no presente contrato ou informações e documentação técnica e não técnica, comercial ou outra, relativa à UMinho, que no âmbito da formação e da execução do contrato, possa ter conhecimento, incluindo os seus agentes, funcionários, colaboradores ou terceiros neles envolvidos, salvo com o consentimento expresso da UMinho.

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 seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

4. O dever de sigilo mantém-se em vigor indefinidamente, até autorização expressa em contrário pela UMinho, a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Cláusula 8.ª
Regulamento de Proteção de Dados

1 – O adjudicatário obriga-se a cumprir o disposto em todas as disposições legais aplicáveis em matéria de tratamento de dados pessoais, no sentido conferido pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ("Regulamento Geral sobre a Proteção de Dados") e demais legislação comunitária e nacional aplicável, em relação a todos os dados pessoais a que aceda no âmbito dos serviços a prestar ao abrigo do contrato a celebrar.

2 – O adjudicatário compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou, por qualquer outra pessoa, colocar à disposição de terceiros os dados pessoais a que tiver acesso ou lhe forem transmitidos pela Universidade do Minho ao abrigo do contrato a celebrar, sem que para tal tenha sido expressamente instruído, por escrito, pela Universidade do Minho ou pelos titulares dos dados no exercício dos seus respetivos direitos.

3 - O adjudicatário obriga-se a pôr em prática as medidas técnicas e de organização necessárias à proteção dos dados pessoais tratados por conta da Universidade do Minho contra a respetiva destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.

4 – As medidas a que se refere o número anterior devem garantir um nível de segurança adequado em relação aos riscos que o tratamento de dados apresenta, à natureza dos dados a proteger e aos riscos, de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares.

5 – O adjudicatário compromete-se a que o acesso aos dados pessoais tratados ao abrigo do contrato a celebrar será estritamente limitado ao pessoal que necessitar de ter acesso aos mesmos para efeitos de cumprimento das obrigações assumidas.

6 – O adjudicatário obriga-se a comunicar à Universidade do Minho qualquer situação que possa afetar o tratamento dos dados pessoais ou de algum modo dar origem ao incumprimento das disposições legais em matéria de proteção de dados, devendo ainda tomar todas as medidas necessárias e ao seu alcance para a fazer cessar de imediato.

7 – O adjudicatário será responsável por qualquer prejuízo em que a Universidade do Minho vier a incorrer em consequência do tratamento, por si ou pelo seu pessoal, de dados pessoais ou em violação das normas legais aplicáveis, quando tal violação seja imputável ao adjudicatário e solidária com o pessoal no âmbito do serviço prestado, quando a violação seja imputável à atuação destes últimos.

Secção II
Obrigações da entidade adjudicante

Cláusula 9.ª
Preço base

1.O preço base do presente procedimento é estabelecido em **9.574,00€ (nove mil quinhentos e setenta e quatro euros**) acrescido de IVA, sendo este o preço máximo que a entidade adjudicante se propõe a pagar por todas as prestações objeto do contrato, nos termos do n.º 1 do artigo 47º do Código dos Contratos Públicos.

2.O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças

3.O preço base resulta dos preços atualizados do mercado obtidos através da consulta preliminar prevista no artigo 35ºA do CCP

Cláusula 10.ª
Preço contratual e condições de pagamento

1.Pela prestação objeto do contrato, bem como pelo cumprimento das demais obrigações constantes no presente caderno de encargos, a entidade adjudicante pagará ao adjudicatário o preço constante da proposta adjudicada, acrescido do IVA à taxa legal em vigor, se este for legalmente devido

2.O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, nomeadamente os relativos ao transporte dos bens objeto do contrato para o respetivo local de entrega, os custos com alojamento, alimentação e deslocação de meios humanos, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças

3. A quantia devida pela Universidade do Minho deve ser paga no prazo de 30 (trinta) dias após a receção da respetiva fatura, que só pode ser emitida após o vencimento da obrigação respetiva e desde que cumpridas as formalidades legais exigidas

4. Para efeito do número anterior, a obrigação considera-se vencida após a prestação de serviços a que respeita, com a emissão da Declaração de Aceitação, referida no n.º 6 da Cláusula 6.ª do presente caderno de encargos, pela Universidade do Minho.

5. Em caso de discordância por parte da Universidade do Minho, quanto aos valores indicados nas faturas, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando a entidade adjudicatária obrigada a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.

6. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas através de transferência bancária.

7. Independentemente do referido nos números anteriores o pagamento a efetuar ao abrigo do contrato só será efetuado depois de verificados todos os formalismos legais a que obedece a despesa pública.

Capítulo III
Incumprimento do contrato

Cláusula 11.ª
Penalidades Contratuais

1 – Pelo incumprimento de obrigações emergentes do contrato, por razões imputáveis ao adjudicatário, confere à Universidade do Minho o direito à aplicação de sanção pecuniária, a fixar em função da gravidade do incumprimento, nos termos do artigo 329.º do CCP, designadamente.

a) se o adjudicatário não cumprir os prazos contratualmente estabelecidos, acrescidos de prorrogações graciosas ou legais, ser-lhe-á aplicada, até à completa disponibilização do bem/prestação dos serviços, ou até à rescisão do contrato, a seguinte multa contratual:

a.1) uma multa diária de 0,5% (meio por cento) do valor da adjudicação, nos primeiros dez dias de atraso.

a.2) uma multa diária de 1% (um por cento) do valor da adjudicação, a partir do décimo primeiro dia de atraso.

2 – Na determinação da gravidade do incumprimento, a Universidade do Minho tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.

3 – A acumulação das penas pecuniárias previstas no presente artigo não pode exceder 20% do preço contratual, sem prejuízo da resolução do contrato nos termos legais.

4 – Nos casos em que seja atingido o limite previsto no número anterior e a Universidade do Minho decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.

5 – Para efeitos dos limites previstos nos n.ºs 3 e 4, quando o contrato previr prorrogações expressas ou tácitas, o valor das sanções a aplicar deve ter por referência o preço do seu período de vigência inicial.
6 – Considera-se haver incumprimento definitivo, suscetível de aplicação da sanção de resolução sancionatória quando, após notificação e concessão de prazo para o cumprimento da obrigação em falta, o adjudicatário continue a incorrer em incumprimento.
7 – A UMinho pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos do presente artigo.
8 – As penas pecuniárias eventualmente aplicáveis ao adjudicatário não obstam a que a UMinho exija uma indemnização pelo dano excedente.
9 – Em caso de atraso da UMinho no cumprimento das suas obrigações pecuniárias, o adjudicatário tem direito aos juros de mora sobre o montante em dívida à taxa legalmente fixada para o efeito pelo período correspondente à mora, nos termos previstos no artigo 326.º do CCP

Cláusula 12.ª
Gestor do Contrato

1 – A UMinho procederá à designação de um ou mais gestores do contrato, com a função de acompanhar permanentemente a execução deste, nos termos e para os efeitos do disposto no artigo 290.º-A do CCP.
2 – Cabe ao gestor do contrato exercer as competências que expressamente decorram da lei, bem como as que lhe sejam atribuídas pela Universidade do Minho, em matéria de acompanhamento da execução e verificação do cumprimento de todas as obrigações legais e contratuais assumidas pelo adjudicatário.
3 – No desempenho das suas funções o Gestor do Contrato tem direito de acesso e consulta a toda a documentação relacionada com as atividades objeto do presente procedimento.
4 – Caso o gestor 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.
5 – O adjudicatário obriga-se a cooperar com o Gestor do Contrato, designado pela Universidade do Minho, na prossecução das atividades de acompanhamento que este tem a seu cargo

Cláusula 13.ª
Revogação do contrato

O presente contrato pode ser revogado, a todo o tempo, por acordo escrito, assinado pelos legais representantes de ambas as partes, do qual deve constar a referência ao presente contrato e seus aditamentos, bem como a data de início da produção de efeitos da revogação.

Cláusula 14.ª
Resolução por parte do contraente público

1 – Sem prejuízo de outros fundamentos de resolução previstos na lei, a Universidade do Minho pode resolver o contrato no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.

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

Cláusula 15.ª
Resolução por parte do adjudicatário

1 – Sem prejuízo de outros fundamentos de resolução previstos na lei, o adjudicatário pode resolver o contrato quando:

a) Qualquer montante que lhe seja devido esteja em dívida há mais de 6 (seis) meses ou o montante em dívida exceda 25% do preço contratual, excluindo juros;

2 – O direito de resolução é exercido por via judicial nos termos da Cláusula 20.ª.

3 - Nos casos previstos na alínea a) do n.º 1, o direito de resolução pode ser exercido mediante declaração enviada à Universidade do Minho, que produz efeitos 30 (trinta) dias após a receção dessa declaração, salvo se esta última 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.

Cláusula 16.ª
Casos fortuitos ou de força maior

1 – Não podem ser impostas penalidades, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar, que se reconduzem expressamente a tremores de terra, inundações, incêndios, epidemias, sabotagens, greves ou outros conflitos coletivos de trabalho, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas, exceto as que resultem de incumprimentos de deveres e normas legais a que está obrigado.

2 – A parte que invoca casos fortuitos ou de força maior deve comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

3 – A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 17.ª
Subcontratação e cessão da posição contratual

O adjudicatário não poderá subcontratar ou ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato, sem autorização prévia e por escrito da UMinho e nos termos do previsto no Código dos Contratos Públicos.

Cláusula 18.ª
Cessão da posição contratual por incumprimento do cocontratante

Em caso de incumprimento, pelo cocontratante, das suas obrigações, que reúna os pressupostos para a resolução do contrato, nos termos da Cláusula 14.ª, o cocontratante deverá ceder a sua posição contratual ao concorrente do procedimento pré-contratual na sequência do qual foi celebrado o contrato em execução, que venha a ser indicado pelo contraente público, pela ordem sequencial daquele procedimento, nos termos e para efeitos do disposto no artigo 318.º-A do CCP.

Cláusula 19.ª
Comunicações e notificações

1 – Sem prejuízo de poderem ser aprovadas 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 domínio 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
Foro Competente

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

Cláusula 21.ª
Legislação aplicável

Em tudo o que não se encontrar especialmente regulado, aplicam-se as disposições constantes do Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, com as atualizações em vigor, e demais legislação específica aplicável.

Parte II – Cláusulas e Especificações Técnicas

Cláusula 22.ª
Âmbito

A Universidade do Minho (UMinho) pretende a aquisição do licenciamento por 1 ano do módulo de cibersegurança endpoint protection para integrar com a solução de firewall Palo Alto que tem atualmente em funcionamento como proteção interna dos serviços críticos alojados no datacenter da UMinho.

Apresentam-se a seguir as especificações técnicas.

Cláusula 23.ª
Especificações técnicas

A Universidade do Minho (UMinho) pretende a aquisição de módulo de segurança endpoint para integrar com a solução de firewall Palo Alto que tem atualmente em funcionamento como proteção interna dos serviços críticos alojados no datacenter da UMinho.

A proposta deverá ter os valores discriminados da mesma forma que o fabricante os apresenta, ou seja, se o fabricante distinguir valores por cada referência de produto (*part-number*), o concorrente deverá refletir essa mesma distinção na proposta.

1	**Requisitos Gerais**
1.1	A instalação de, pelo menos, 200 postos de trabalho/servidores (endpoints) pelo período de um ano
1.2	Prevenção contra exploits, incluindo aqueles que utilizam vulnerabilidades do tipo Zero-Day.
1.3	Prevenção contra a execução de malware, sem requerer qualquer conhecimento prévio.
1.4	Garantir uma análise forense detalhada dos ataques prevenidos.
1.5	Capacidade de restringir a execução de determinados ficheiros.
1.6	Proteger contra ransomware.
1.7	Conseguir prevenir de forma efetiva Exploits e Malwares quando não existe conectividade ou atualizações do servidor de gestão e/ou acesso a recursos da cloud.
1.8	Controlar dispositivos USB
1.9	Disk Encryption
1.10	Host Firewall
1.11	Permitir isolar automaticamente da rede máquinas infetadas com malware
1.12	Módulo de Endpoint Detection and Response (EDR)
2	**Gestão**
2.1	A solução proposta deve ser gerida através de uma interface gráfica web.

2.2	A solução proposta deve poder exportar os seus logs em formato syslog para qualquer solução de gestão de logs.
2.3	A solução proposta deve ter uma gestão centralizada baseada em cloud.
2.4	A solução deve vir de base já configurada com as best practices do fabricante de forma a simplificar o deployment da mesma.
2.5	A solução deve permitir que seja utilizado um serviço de logging na cloud para alojar tanto os logs de firewalls como de endpoints para depois poder integrar com vários outros fabricantes através de uma Framework e APIs.
2.6	A solução proposta deve possuir um modelo de licenciamento por endpoint e/ou largura de banda e não por outros parâmetros como por exemplo número de utilizadores, CPUs, etc.
2.7	A solução proposta deve suportar a atualização de software dos agentes de endpoint diretamente a partir da cloud.
3	**Prevenção de Exploits**
3.1	A solução proposta deve suportar proteger processos do sistema operativo e aplicações, com a capacidade de adicionar à lista de aplicações protegidas, aplicações proprietárias, de terceiras partes ou customizadas.
3.2	A solução proposta deve ser capaz de fornecer prevenção em tempo real contra exploits de qualquer vulnerabilidade aplicacional (incluindo do tipo zero-day ou desconhecidos) através do bloqueio de técnicas de exploits como “Software Logic Flaws”, “Memory Corruptions”, “DLL Hijacking”, “heap spray”, “JIT”, “ROP”, “SEH”, etc.
3.3	A solução proposta deve ser capaz de efetuar prevenção de exploits através do bloqueio de técnicas de exploits sem requerer conectividade com o servidor de gestão e/ou serviço da cloud e sem utilizar assinaturas.
3.4	Assim que a solução proposta previne ou bloqueia uma técnica de exploit deve parar imediatamente o processo relacionado, coletar informação forense (nome do processo, ficheiro de origem e o caminho, data e hora, dump da memória, versão do sistema operativo, identificação do utilizador, identificação e versão da aplicação vulnerável, etc.) e terminar apenas este processo.
3.5	A solução proposta deve utilizar módulos de técnicas de exploit para prevenir ou bloquear exploits. Não deve basear a prevenção ou bloqueio de exploits em assinaturas, reputação e heurísticas dos ficheiros.
3.6	A solução proposta não deve utilizar de forma intensiva os recursos do endpoint ou utilizar técnicas de análise baseada em hardware específico como sandbox local baseado em virtualização de software ou containers. A solução proposta deve ter impacto mínimo no desempenho através da utilização de um agente leve e não intrusivo que pode ser totalmente invisível para o utilizador.
3.7	A solução proposta deve proteger de forma simultânea todas as aplicações e processos do endpoint contra técnicas de exploit.
3.8	A solução proposta deve permitir a configuração granular de políticas de prevenção e bloqueio de exploits por utilizador, grupos ou máquina (endpoint) e ter políticas pré-configuradas para os processos mais comuns do sistema Microsoft Windows.
3.9	A solução proposta deve conseguir proteger o endpoint contra “Kernel privilege escalation”.
3.10	A solução proposta deve também conseguir proteger contra exploits para MacOS e Linux como por exemplo “local privilege escalation”
4	**Prevenção de Malware**
4.1	A solução proposta deve suportar proteção contra a execução de executáveis maliciosos.
4.2	A solução proposta deve garantir a funcionalidade de monitorização ou aprendizagem do ambiente onde está instalado (i.e. processos e aplicações instaladas e a correr nos endpoints). Esta deverá ser utilizada na fase inicial de instalação e configuração.

4.3	A solução proposta deve ter a capacidade de controlar o que pode ser executado no endpoint, a partir de onde pode ser executado e com que parâmetros.
4.4	A solução proposta deve prevenir um processo de lançar qualquer processo legítimo que possa ser utilizado para fins maliciosos. Esta técnica é muitas vezes utilizada em ransomware e outros malwares para fazer bypass à segurança do endpoint.
4.5	A solução proposta deve ser capaz de bloquear processos filhos iniciados por um determinado processo através de whitelist (bloquear todos exceto os listados) e blacklist (bloquear apenas os listados).
4.6	A solução proposta deve ser capaz de prevenir a execução de malware através da análise de comportamentos desencadeados pelo malware.
4.7	A solução proposta deve garantir a possibilidade de configurar whitelists globais para permitir a execução de certos ficheiros executáveis.
4.8	A solução proposta deve ser capaz de criar regras de exclusão das capacidades de proteção para endpoints específicos.
4.9	A solução proposta deve detetar e bloquear malware através do uso de machine learning e não deve utilizar assinaturas locais independentemente do sistema operativo
4.10	A solução deve ser capaz de analisar ficheiros do tipo mach-o, ELF e APK.
4.11	A solução proposta deve ter a opção de integrar com soluções de Advanced Persistent Threat (APT) na cloud, tendo a capacidade de fornecer uma prevenção efetiva mesmo quando não possui ligação à cloud ou ao serviço de gestão centralizado. A solução de APT na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração.
4.12	A solução proposta deve conseguir perguntar aos serviços APT na cloud por valores de hash para verificar se determinado ficheiro é malicioso ou benigno.
4.13	A solução deve utilizar técnicas locais de machine learning para detetar malware desconhecido
4.14	A solução deve monitorizar os diferentes processos bem como as suas relações e origens (Parent processes) de forma a ser capaz de bloquear processos com comportamento malicioso.
5	**Requisitos técnicos obrigatórios**
5.1	A solução proposta deve ter a capacidade de submeter aos serviços APT na cloud ficheiros potencialmente maliciosos.
5.2	A solução proposta deve conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do malware.
5.3	A solução proposta não deve analisar ficheiros que já tenham sido anteriormente submetidos aos serviços APT na cloud.
5.4	A solução proposta deve conseguir prevenir malware desconhecido utilizando tecnologia APT sandbox na cloud e fornecer um relatório com o veredicto e análise do ficheiro submetido. A solução de APT sandbox na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração.
5.5	A solução proposta deve ter a capacidade de modificar manualmente a decisão tomada pelos serviços APT na cloud para uma hash em particular.
5.6	A solução proposta deve ter a capacidade de prevenir a execução de um ficheiro no caso da sua hash ser desconhecida dos serviços APT na cloud.
5.7	A solução proposta deve ter a capacidade de prevenir a execução de um ficheiro no caso do endpoint não conseguir contactar os serviços APT na cloud e o valor da hash do ficheiro não ser localmente conhecido.
5.8	A solução proposta deve garantir a capacidade de efetuar análises estáticas (machine learning) em modo offline para Windows, Linux e macOS.
5.9	A solução proposta deve prevenir processos que corram no endpoint de fazer o carregamento de DLL's maliciosos. A solução proposta deve examinar os DLL's e criar um veredicto sobre se deve ou não ser executado o carregamento de determinado DLL.

5.10	A solução proposta deve conseguir analisar comportamentos de ransomware antes da execução do mesmo e deve conseguir parar ataques baseados em encriptação através da análise em tempo real de atividades de encriptação.
5.11	A solução proposta deve conseguir prevenir ataques que tirem partido do kernel para carregar e correr código "shell" malicioso.
5.12	A solução proposta deve conseguir que o módulo de análise de comportamentos de ransomware opere em modo de notificação ou de prevenção.
5.13	A solução proposta deve possuir um módulo de análise de comportamentos de ransomware que suporte os seguintes sistemas de ficheiros: NTFS, FAT, exFAT.
5.14	A solução deve poder bloquear qualquer dispositivo USB externo que se conecte a um endpoint monitorizado pela solução. Deve ser possível bloquear determinado tipo de dispositivo USB, mas permitir apenas dispositivos de um vendedor específico ou com um Serial Number específico. Deverá ser possível criar políticas apenas temporárias.
5.15	A solução proposta deve ter a capacidade de automaticamente criar uma regra de exclusão e um hash de exclusão a partir do relatório de ameaças detetadas, para garantir que determinado processo possa ser executado num endpoint em particular.
5.16	A solução deve suportar os seguintes sistemas operativos: 1. Android 5, 6, 7, 8, 9 e 10 2. Debian 8 e 9 3. CentOS 6 e 7 4. Oracle 6 e 7 5. Red Hat 6 e 7 6. SUSE 12 7. Ubuntu 12, 14, 16 e 18 8. macOS 10.11, 10.12, 10.13, 10.14 e 10.15 9. Windows 7, 8 e 10 10. Windows Server 2008R2, 2012, 2016 e 2019
5.17	A solução deve suportar ainda os seguintes ambientes virtuais: Citrix XenApp, Citrix App layering, VMware AppVolumes, Vmware ThinApp.
6	**Deteção e Resposta a incidentes**
6.1	A solução deve monitorizar todos os endpoints, nomeadamente informação relativa a: processos, ficheiros, tráfego de rede, registry e memória. Qualquer atividade relacionada com estes pontos deve ser guardada no mínimo para os últimos 30 dias. Deverá ser possível prolongar esta retenção indefinidamente.
6.2	Com base na informação disponível para os últimos 30 dias, a solução deve ser capaz de detetar máquinas comprometidas, seja com base em análise de processos, ficheiros, registry, e tráfego de rede nas máquinas ou com base na análise do comportamento do utilizador ligado na máquina.
6.3	A solução deve permitir ao analista definir regras e pesquisar por padrões relacionados com toda a informação que é retida para os endpoints. Por exemplo, deve ser possível pesquisar por endpoints onde determinada registry key foi modificada. Isto sem ser necessário utilizar ou aprender uma nova query language.
6.4	Quando diferentes alertas estão relacionados, a solução deve ser capaz de os agregar automaticamente em um único incidente.
6.5	Deve ser possível agregar diferentes incidentes num único.
6.6	Quando é identificado um novo incidente, a solução deve ser capaz de automaticamente identificar a root cause do incidente e mostrar toda a sequência de eventos que causou o incidente, assim como todas as alterações introduzidas por estes eventos. Para cada evento deve ser possível visualizar o processo associado, o tráfego de rede gerado por esse processo,

	os ficheiros acedidos alterados ou criados, qualquer modificação no registry, assim como todos os módulos/DLLs carregados por este processo em memória.
6.7	Para cada incidente, a solução deve indicar: todos os alertas associados a este incidente, todos os artefactos relevantes para a investigação, as máquinas e os utilizadores envolvidos. Cada incidente deve ter uma funcionalidade de chat e de notas para os analistas poderem colaborar entre si.
6.8	Para cada artefacto deve existir informação sobre se há assinaturas válidas para estes, assim como um veredicto sobre o artefacto da própria cloud do fabricante assim como de ferramentas OpenSource (ex:VirusTotal)
6.9	A solução deve mapear os diferentes alertas para a Framework Mitre ATT&CK
6.10	Através de licenciamento adicional, a solução deve ser capaz de ingerir dados da rede do cliente (on-prem e cloud) de forma a ter visibilidade de todo o tráfego de rede e efetuar deteção comportamental sobre a rede, endpoint e cloud numa única solução e interface gráfica. Para recolher o tráfego de rede a solução deve ser capaz de integrar com pelo menos 4 fabricantes de Firewalls.
6.11	Através de licenciamento adicional deve ser possível ingerir logs de identity providers, nomeadamente: AzureAD, Okta e PingID de forma a detetar anomalias nos padrões de autenticação dos utilizadores.
6.12	Deve existir uma funcionalidade de "search&destroy" que permite pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo
6.13	A solução deve aprender o comportamento de cada máquina e criar perfis de forma a ser capaz de identificar comportamentos anômalos
6.14	Com base na aprendizagem comportamental para cada máquina e utilizador a solução deverá ser capaz de gerar alarmística para estes cenários: 1. Sessão rara de SSH 2. Uso de comandos fora do comum (arp -a, ipconfig, etc) 3. processos raros a comunicar com máquinas fora da organização 4. processos a comunicar com máquinas externas que não são normalmente acedidas pelas máquinas da organização 5. scripts a comunicar com hosts externos 6. listagem de utilizadores do domínio 7. comando de powershell anormal 8. volume de conexões entre máquinas elevado
6.15	Capacidade de reverter automaticamente alterações feitas na máquina por determinado malware. A solução deve listar as alterações feitas por qualquer processo malicioso e permitir reverter essas alterações.
7	**Visiblidade sobre as máquinas**
	A solução deve permitir adicionar no futuro (através de licenciamento adicional) um módulo de visibilidade com as seguintes características:
7.1	Capacidade de identificar: 1. Utilizadores e grupos configurados em cada máquina 2. Serviços a correr nas máquinas 3. Drivers instalados nas máquinas 4. Processos, drivers, serviços que são automaticamente inicializados sempre que o utilizador liga as máquinas. 5. Shares de rede configurados nas máquinas 6. Discos existentes nas máquinas
7.2	Funcionalidade de "search&destroy" que permite pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo

7.3	Identificar vulnerabilidades e respetiva criticidade para ambientes Windows e Linux
7.4	Identificar as aplicações a correr em cada equipamento
8	**Resposta a incidentes**
8.1	A solução proposta deve permitir iniciar scans de malware à máquina infetada.
8.2	Deve ser possível efetuar blacklists e whitelists a hashes.
8.3	Deve ser possível fazer quarentena a determinados processos.
8.4	Durante a investigação de um incidente, a solução deve permitir isolar da rede máquinas infetadas.
8.5	A solução deve permitir reverter automaticamente alterações que tenham sido efetuadas por um processo malicioso. Exemplo: Alterar uma registry key para o valor anterior ao comprometimento da máquina.
8.6	Deve existir uma funcionalidade de Live Terminal, onde o analista possa aceder remotamente às máquinas de forma a: gerir os processos e ficheiros, correr scripts python, correr comandos de Powershell e aceder à linha de comandos da máquina.
8.7	Deve ser possível correr scripts em python sobre todo o parque de máquinas instalado em simultâneo. A solução deve disponibilizar scripts para os use cases mais comuns e permitir a criação de novos scripts.
8.8	Capacidade de criar regras de correlação personalizadas que permitem detetar ataques retroativamente.
8.9	A solução deve incluir uma linguagem de consulta avançada que suporte wildcards, expressões regulares, JSON, agregação de dados, manipulação de campos e valores, agregação de dados de fontes diferentes e visualização de dados.
9	**Análise Forense**
	A solução deve permitir adicionar no futuro (através de licenciamento adicional), um módulo forense com as seguintes características:
9.1	Identificar a atividade do atacante através da revisão dos principais artefactos obtidos do endpoint, como logs de eventos, chaves de registo, histórico do browser, etc;
9.2	Obter informação detalhada do sistema como lista completa de ficheiros de todas as drives, incluindo drives removidas;
9.3	Permitir o download de um snapshot forense completo do endpoint, e o upload do mesmo para a solução para análise;
9.4	Recolha de dados: 1. Histórico do browser: Chrome; Edge; Firefox; Internet Explorer 2. Acesso a ficheiros: Recent files (LNK files); Jump lists; OpenSavePidlMRU; ShellBags; WordWheelQuery 3. Processos executados: Amcache; Application Resource Usage (SRUM); Background Activity Monitor; CIDSizeMRU; LastVisitedPidlMRU; Prefetch; RecentFileCache; Shimcache; UserAssist; Windows Timeline 4. Actividade de rede: ARP cache; DNS cache; Hosts File; Network Connectivity Usage (SRUM); Network Data Usage (SRUM) 5. Acessos remotos: LogMeIn; TeamViewer 6. Histórico de comandos: PSReadLine 7. Triagem: File listing ($MFT); Registry listing; Event logs; Net sessions; Handle listing