REPÚBLICA PORTUGUESA
EDUCAÇÃO

IAVE INSTITUTO DE AVALIAÇÃO EDUCATIVA, I.P.

Aprovo.

Luís Miguel Pereira dos Santos

Assinado de forma digital por Luís Miguel Pereira dos Santos
DN: c=PT, title=Presidente do Conselho Diretivo do IAVE, ou=Conselho Diretivo, o=Instituto de Avaliação Educativa IP, sn=Pereira dos Santos, givenName=Luís Miguel, cn=Luís Miguel Pereira dos Santos
Dados: 2023.06.29 16:01:55 +01'00'

CONCURSO PÚBLICO INTERNACIONAL N.º CPI/01/ 2023

CADERNO DE ENCARGOS nº 9/IAVE/2023

Aquisição de Endpoints , Display's e Pacote de software de segurança

Classificação CPV: 30213300-6 - Computadores portáteis
30231310-3 - Visores de painel plano
48730000-4 – Pacote de software de segurança

PARTE I – Cláusulas Jurídicas

Artigo 1. º
Objeto

1. O objeto do presente Caderno de encargos é a aquisição para o Instituto de Avaliação Educativa, I.P. (doravante IAVE, I.P.) de:

Tipo	Descrição	Quantidade
Endpoint tipo 1	Endpoint Básico	200
Endpoint tipo 2	Endpoint Avançado	150
Display	Monitor 23.8"	200
Segurança de dispositivos	Segurança de dispositivos	300

2. Consideram-se, nomeadamente, abrangidos pelo objeto do presente procedimento, a execução de todas as prestações inerentes aos serviços pós-venda, de acordo com as especificações descritas no artigo 23.º presente Caderno de Encargos.

Artigo 2. º
Forma e documentos contratuais

1. O contrato a celebrar integra os seguintes elementos:
   a) O presente caderno de encargos
   b) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelas entidades convidadas, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;

c) Os esclarecimentos e as retificações relativos ao caderno de encargos;
d) A proposta adjudicada;
e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

2. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem que nele se dispõe, sem prejuízo da aplicação do princípio da prevalência revisto no seu artigo 51º do Código dos Contratos Públicos, doravante apenas CCP.
3. Em caso de divergência entre os documentos referidos no número 2 e o clausulado do contrato e seus anexos prevalecem os primeiros, salvo quanto aos ajustamentos propostos, de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário, nos termos do disposto no artigo 101º desse mesmo diploma.
4. Além dos documentos referidos no n.º 2, o adjudicatário obriga-se igualmente a respeitar, no que lhe seja aplicável, as normas europeias e portuguesas, as especificações e homologações de organismos oficiais e fabricantes ou entidades detentoras de patentes.

Artigo 3. º
Boa-fé

As partes obrigam-se a atuar de boa-fé na execução do contrato e a não exercer os direitos nele previstos, ou na lei, de forma abusiva.

Artigo 4. º
Local, forma e período de execução do contrato

1. O contrato que vier a ser celebrado vigorará nos termos previstos no seu clausulado, devendo ser executado no período máximo de 60 (sessenta) dias após a receção e validação da conformidade dos equipamentos pelo IAVE e entendendo-se por execução a implementação de configuração e instalação da componente de segurança, nos diversos equipamentos, sem prejuízo do estabelecido no artigo 45º da Lei n.º 98/97, de 26 de agosto a Lei de Organização e Processo do tribunal de Contas, quanto à produção de efeitos dos contratos sujeitos à fiscalização prévia do Tribunal de Contas.
2. Os bens objeto do contrato deverão ser disponibilizados, nas instalações do Instituto de Avaliação Educativa, sitas na Travessa Terras de Sant'Ana, 15,1250-269 Lisboa, até 120 dias após adjudicação.

Artigo 5.º
Preço base

1. O preço base, estabelecido de acordo com o artigo 47º do CCP, é de 840.120,00 € (oitocentos e quarenta mil cento e vinte euros), valor ao qual acresce o IVA à taxa legal em vigor. A fixação do presente preço base tem como fundamento os preços de mercado praticados em procedimentos anteriores referentes aos equipamentos que se pretendem adquirir, nomeadamente:

Equipamento	Quantidade	Preço unitário	Total
Endpoint 1	200	1 950,00 €	390 000,00 €
Endpoint 2	150	2 150,00 €	322 500,00 €
Display	200	338,10 €	67 620,00 €
Segurança	300	200,00 €	60 000,00 €
Preço base			840 120,00 €

Artigo 6. º
Condições de pagamento

1. As quantias devidas pelo IAVE no âmbito do contrato serão pagas nos termos constantes nos números seguintes.
2. Os pagamentos serão realizados, no prazo máximo de 60 (sessenta) dias após a aceitação dos bens e verificação da sua conformidade pelo IAVE, I. P., e a receção das respetivas faturas.
3. Não são, em caso algum, concedidos adiantamentos.
4. Em caso de discordância por parte do IAVE, I.P., quanto aos valores indicados nas faturas, deve comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
5. As faturas devem conter obrigatoriamente o n.º de compromisso gerado pela entidade adjudicante, nos termos da lei, bem como descrever o bem.
6. Desde que regularmente emitidas, e observado o disposto nos números precedentes, as faturas são pagas através de transferência bancária para o IBAN indicado pelo adjudicatário, mediante preenchimento da ficha de fornecedor, sem prejuízo do que resulta da submissão deste contrato ao visto do tribunal de contas.

Artigo 7. º
Obrigações do adjudicatário

1. São obrigações do adjudicatário, além de outras decorrentes do estabelecido nas peças do presente procedimento e na legislação aplicável, os que seguidamente se enunciam e que devem ser objeto de cláusulas específicas a incluir no contrato a celebrar:

    a) Assegurar a entrega dos bens e a execução de todas as obrigações contratuais, conforme definido no presente caderno de encargos e seus anexos, bem como nos demais documentos contratuais;
    b) Comunicar, antecipadamente, ao IAVE, I.P., qualquer facto que torne total ou parcialmente impossível a entrega de qualquer dos bens objeto do presente procedimento, ou implique o incumprimento de qualquer outra das suas obrigações;
    c) Alterar as condições subjacentes à prestação de serviço acordada entre as partes, através da celebração de contrato escrito entre as mesmas, apenas com prévia autorização escrita da entidade adjudicante;
    d) Assegurar todos os meios humanos e materiais que se demonstrem necessários e indispensáveis à execução do contrato;
    e) Assegurar, de forma correta e fidedigna, as informações referentes às condições em que a prestação dos bens será executada, disponibilizando todos os esclarecimentos que se justifiquem e no prazo indicado pelo IAVE, I.P.;
    f) Comunicar qualquer facto que, ocorrendo durante a execução do contrato, se demonstre relevante para a normal prestação dos bens e para a execução contratual, nomeadamente, a alteração da denominação social ou dos seus representantes legais.

Artigo 8. º
Patentes, licenças e marcas registadas

São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização de marcas registadas, patentes registadas, licenças ou outros direitos similares.

Artigo 9. º
Uso de sinais distintivos

Nenhuma das partes pode utilizar a denominação, marcas, nomes comerciais, logótipos e outros sinais distintivos do comércio que pertençam à outra sem o seu prévio consentimento escrito.

Artigo 10. º
Sigilo

1. O adjudicatário garantirá o sigilo quanto a quaisquer informações de que venham a ter conhecimento relacionadas com a atividade do IAVE, I.P., em virtude da aquisição dos bens objeto do presente contrato.
2. Excluem-se do dever de sigilo previsto no número anterior, a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo prestador de bens ou que este seja obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Artigo 11. º
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 ou para efeitos da prestação dos Bens, nomeadamente, dados pessoais de clientes, trabalhadores, colaboradores e prestadores de bens do IAVE, I.P.
2. As partes reconhecem e aceitam que, relativamente a todos os dados pessoais a que o adjudicatário tiver acesso ou lhe forem transmitidos pelo IAVE, I.P. para efeitos da prestação dos Bens:
   a) O IAVE, I.P. atuará na qualidade de responsável pelo tratamento dos dados (tal como definido no Regulamento Geral sobre a Proteção de Dados), determinando as finalidades e os termos do tratamento desses dados pelo adjudicatário;
   b) O adjudicatário atuará na qualidade de entidade subcontratante (tal como definido no Regulamento Geral sobre a Proteção de Dados), tratando os dados pessoais em estrita observância das instruções da responsável pelo tratamento desses dados;
   c) Entende-se, para este efeito, que tratamento de dados pessoais são as operações, com ou sem recurso a meios automatizados, efetuadas sobre os dados pessoais dos trabalhadores do IAVE, I.P., incluindo a recolha, o registo, a organização, o armazenamento, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a divulgação, a transferência e/ou a disponibilização a terceiros, o alinhamento, a combinação, o bloqueamento, o apagamento e a destruição dos dados suprarreferidos;
3. 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 responsável dos tratamentos de dados ao abrigo do presente Contrato, sem que para tal tenha sido expressamente instruído, por escrito, por aquela responsável ou pelos titulares dos dados no exercício dos seus respetivos direitos.

4. Sem prejuízo das demais obrigações previstas no presente Contrato, o adjudicatário obriga-se a cumprir rigorosamente o disposto na legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:
   a) Tratá-los apenas de acordo com as instruções do IAVE, I.P., única e exclusivamente, para efeitos da presente prestação dos bens, cumprindo-se as obrigações estatuídas sobre proteção de dados;
   b) Prestar toda a colaboração de que este careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais efetuado ao abrigo do presente Contrato e manter o IAVE, I.P. informado em relação ao tratamento de dados pessoais;
   c) Prestar assistência ao IAVE, I.P. , tendo em conta a natureza do tratamento e a informação ao seu dispor, no sentido de assegurar as obrigações referentes à notificação de violações de dados pessoais, designadamente através da comunicação sempre que que possível até 72 horas subsequentes ao conhecimento (da ocorrência) de qualquer violação de dados pessoais que ocorra, prestando ainda colaboração ao IAVE, I.P. na adoção de medidas de resposta ao incidente, na investigação do mesmo e na elaboração das notificações que se mostrem necessárias nos termos da lei;
   d) Colaborar com o IAVE, I.P. tendo em conta a natureza do tratamento e, na medida do possível adotar as medidas técnicas e organizativas referidas nesta Cláusula, onde se incluem a cifragem ou a pseudonimização aos dados pessoais para reduzir os riscos para os titulares de dados em questão, não excluindo outras eventuais medidas de proteção de dados, e permitindo-se que estas cumpram a sua obrigação de dar resposta aos pedidos dos titulares dos dados, tendo em vista o exercício, por estes, dos seus direitos nos termos da lei;
   e) Não comunicar dados pessoais a terceiros e a prestadores de bens não autorizados ou não indicados pelo IAVE, I.P.;
   f) Consoante a escolha do IAVE, I.P. ou do titular eliminar ou devolver os dados pessoais no momento da cessão do Contrato, apagando e destruindo quaisquer cópias existentes, exceto se a conservação ou a transmissão dos dados for exigida por lei;
   g) Manter registos das atividades de tratamento de dados realizadas em nome do IAVE, I.P. ao abrigo do presente Contrato, segundo os requisitos previstos na lei;
   h) Cumprir todas as demais disposições legais no que respeita ao registo, transmissão ou qualquer outra operação de tratamento de dados pessoais previstas na lei;
   i) Não os transferir para fora do Espaço Económico Europeu, sem o consentimento prévio por escrito da responsável pelo tratamento dos dados;
   j) Disponibilizar ao responsável pelo tratamento dos dados todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na lei no respetivo âmbito e facilitar e contribuir para as auditorias, inclusive as inspeções conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado;
   k) Assegurar que o pessoal autorizado a tratar de dados pessoais assume um compromisso de confidencialidade e que conhece e se compromete a cumprir todas as obrigações aqui previstas.
5. O adjudicatário obriga-se a pôr em prática as medidas técnicas e de organização necessárias à proteção dos dados pessoais tratados por conta do IAVE, I.P., 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.

6. 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.
7. O adjudicatário concorda com o acesso aos dados pessoais tratados ao abrigo do presente Contrato será estritamente limitado ao pessoal que necessitar de ter acesso aos mesmos para efeitos de cumprimento das obrigações aqui assumidas pelo adjudicatário.
8. O adjudicatário obriga-se a comunicar ao responsável pelo tratamento dos dados 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.
9. O adjudicatário será responsável por qualquer prejuízo em que o IAVE, I.P. vier a incorrer em consequência do tratamento, por si ou pelo seu pessoal, de dados pessoais ou em violação das normas legais aplicáveis e ao disposto no presente Contrato, 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.
10. O adjudicatário, sempre que o IAVE, I.P. receber um pedido de acesso ou retificação de dados pessoais ou uma oposição ao seu tratamento por parte dos seus titulares dos dados, deverá prestar assistência à responsável pelo tratamento dos dados através de medidas técnicas e organizativas adequadas, para permitir que esta cumpra a sua obrigação de dar resposta aos pedidos dos titulares, tendo em vista o exercício dos seus direitos legais.

Artigo 12. º
Alterações ao contrato

1. O contrato pode ser alterado, de acordo com os artigos 311º e 312º, ambos do CCP, nomeadamente, por:
   a) Acordo das partes, que não pode revestir forma menos solene do que a do contrato;
   b) Alteração anormal e imprevisível das circunstâncias em que as partes tenham fundado a decisão de contratar, desde que a exigência das obrigações por si assumidas afete gravemente os princípios da boa-fé e não esteja coberta pelos riscos próprios do contrato;
   c) Razões de interesse público decorrentes de necessidades novas ou de uma nova ponderação das circunstâncias existentes, sem prejuízo das indeminizações a que houver lugar, nos termos da lei.

Artigo 13. º
Cessão da posição contratual

2. O adjudicatário não poderá ceder a sua posição contratual sem autorização prévia do IAVE, I.P.
3. O adjudicatário, será autorizado a recorrer à subcontratação de um terceiro para colaboração na prestação dos bens, desde que se assegure que o mesmo cumprirá o disposto na legislação aplicável, devendo tal obrigação constar de contrato escrito que, para o efeito, se obriga a celebrar com esse terceiro em que este se vincula ao cumprimento das obrigações decorrentes do Regulamento (UE) 2016/679 e demais legislação aplicável relativa a Dados Pessoais, vinculando suas ações à essência, natureza e finalidades da presente disposição contratual, no estrito cumprimento do dever de sigilo e de confidencialidade.
4. Para efeitos da autorização prevista no número anterior, deve ser apresentada pelo cessionário toda a documentação exigida ao adjudicatário no presente procedimento, para verificação pelo

IAVE IP. de que o cessionário não se encontra em nenhuma das situações previstas no artigo 55.º do CCP e que a cessão não altera as circunstâncias do cumprimento das obrigações contratuais e legais.

Artigo 14. º
Resolução do Contrato

1. O incumprimento por uma das partes dos deveres resultantes do contrato confere, nos termos previstos no regime jurídico aplicável, à outra parte, o direito a resolver o contrato, sem prejuízo das correspondentes indemnizações legais e dos demais fundamentos gerais de resolução do contrato legalmente previstos.
2. Para efeitos do disposto no número anterior, considera-se existir incumprimento definitivo quando houver atraso na prestação por período superior a 10 dias úteis.
3. A resolução será efetuada mediante aviso prévio, através de carta registada com aviso de receção, enviada com a antecedência mínima de 10 dias úteis, contados a partir da data do que se considera ser o incumprimento de definitivo, previsto no número anterior, deste mesmo artigo.
4. A resolução do contrato não prejudica a aplicação de quaisquer sanções pecuniárias, nos termos do artigo seguinte.

Artigo 15. º
Penalidades

1. No caso de não cumprimento das obrigações contratuais, a entidade adjudicante pode aplicar ao adjudicatário as seguintes sanções contratuais pecuniárias, em função da gravidade ou reiteração da infração:
    a) Pelo incumprimento das obrigações relativas ao dever de confidencialidade, até 1000,00€ (mil euros), por infração;
    b) Pelo incumprimento das obrigações relativas à propriedade intelectual e dados pessoais, até 1000,00€ (mil euros), por infração;
    c) Pelo incumprimento dos deveres de informação até 250,00€ (duzentos e cinquenta euros), por infração;
    d) Pelo incumprimento da determinação que seja dirigida ao adjudicatário nos termos do presente Caderno de Encargos, nas quais se incluem as obrigações previstas na Cláusula 1.ª, até 250,00€ (duzentos e cinquenta euros), por infração;
    e) Pelo incumprimento das obrigações acima elencadas, poderão ser aplicadas as referidas penalidades, não excedendo os 20% ou 30% do montante total adjudicado, consoante os casos e, de acordo com o previsto no artigo 329.º do Código dos Contratos Públicos.
2. O pagamento das eventuais penalidades em que o adjudicatário incorra será deduzido do valor líquido da faturação da segunda outorgante.
3. A aplicação das penalidades previstas na presente cláusula será objeto de audiência prévia, nos termos previstos no n.º 2 do artigo 308.º do Código dos Contratos Públicos.

4. O adjudicatário será notificado, por escrito, para que no prazo de 10 (dez) dias úteis se pronuncie. Caso o adjudicatário não se pronuncie no prazo concedido, a entidade adjudicante aplica a penalidade de acordo com o n.º 2 da presente Cláusula.

Artigo 16. º
Mora da entidade adjudicante

1. O atraso em qualquer pagamento não determina o vencimento das restantes obrigações de pagamento.
2. Em caso de mora, os pagamentos devidos pela entidade adjudicante vencem juros, à taxa legal, desde a data em que se tornaram exigíveis e até integral pagamento, nos termos do artigo 326.º do Código dos Contratos Públicos.
3. Em caso de desacordo sobre o montante devido, deve o contraente público efetuar o pagamento sobre a importância em que existe concordância do cocontratante.
4. Os valores contestados pela entidade adjudicante e que vierem a ser objeto de correção não vencem juros de mora em caso de não pagamento.

Artigo 17. º
Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, for impedida de cumprir as obrigações assumidas no contrato, 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.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, sismos, 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) Greves ou conflitos laborais limitados às sociedades da segunda outorgante ou a grupos de sociedades em que esta se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
    b) Circunstâncias que não constituam força maior para os subcontratados da segunda outorgante, na parte em que intervenham;
    c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pela segunda outorgante de deveres ou ónus que sobre ela recaiam;
    d) Manifestações populares resultantes do incumprimento, pela segunda outorgante, de normas legais;

e) Incêndios ou inundações com origem nas instalações da segunda outorgante cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;

f) Avarias nos sistemas informáticos ou mecânicos da segunda outorgante não devidas a sabotagem;

g) Eventos que estejam ou devam estar cobertos por seguros.

4. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar de imediato tais situações à outra parte, por qualquer meio escrito, bem como informar o prazo previsível para restabelecer a situação.

5. 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.

Artigo 18. º

Contagem dos prazos na fase de execução do contrato

À contagem de prazos na fase de execução do contrato a celebrar na sequência do presente procedimento, são aplicáveis as seguintes regras:

a) Os prazos são contínuos, não se suspendendo nos sábados, domingos e feriados;

b) O prazo que termine em sábado, domingo, feriado ou em dia em que o serviço, perante o qual deva ser praticado o ato, não esteja aberto ao público, ou não funcione durante o período normal, transfere-se para o 1.º dia útil seguinte.

Artigo 19. º

Celebração do contrato escrito

De acordo com o disposto nº 1 do artigo 94º do Código dos Contratos Públicos o contrato será reduzido a escrito.

Artigo 20. º

Comunicações e notificações

1. Todas as notificações e comunicações entre a entidade adjudicante e a entidade adjudicatária deverão ser efetuadas por escrito, através de correio, correio eletrónico ou de telecópia, para o domicílio ou sede contratual de cada uma, identificado no contrato, com suficiente clareza, para que o destinatário fique ciente da respetiva natureza e conteúdo.
2. Qualquer alteração das informações de contato constantes do contrato, mesmo que pontuais ou temporárias, devem ser comunicadas de imediato e por escrito à outra parte.

Artigo 21. º

Fundamentação da decisão do procedimento

1. O presente procedimento concurso público internacional é adotado nos termos do disposto na alínea a) do artigo 20.º e artigo 130.º e seguintes do CCP, do Código dos Contratos Públicos e a decisão de contratar foi tomada pelo Presidente do Conselho Diretivo Dr. Luís Pereira dos Santos.

Artigo 22. º

Foro competente

1. Em tudo o que o presente caderno de encargos for omisso observar-se-á o disposto no CCP, e demais legislação e regulamentação aplicável.

2. Para o conhecimento de quaisquer litígios emergentes do presente procedimento e do contrato, designadamente relativas à respetiva interpretação, execução, incumprimento, invalidade, resolução ou redução, é competente o foro da comarca de Lisboa.

Parte II

Especificações técnicas

Artigo 23.º
Especificações técnicas dos equipamentos

1. As especificações técnicas dos equipamentos objeto do presente caderno de encargos, estão descriminados conforme as seguintes especificações (O símbolo “>=” significa maior ou igual, ou seja, que as quantidades referidas são as mínimas necessárias, sendo possível a apresentação de quantidades superiores).

- **Endpoint Básico**

REQ	Requisito	Requisito Obrigatório
Processador		
1	12th Generation Intel® Core™ i7-1255U Processor (E-cores up to 3.50 GHz P-cores up to 4.70 GHz) ou equivalente	x
Sistema Operativo		
2	Windows 11 Pro 64 Portuguese/English	x
Ecrã		
3	Capacidade de suporte até 4 displays (display nativo e 3 displays externos via HDMI, USB-C e Thunderbolt)	x
4	HDMI suporte até 3840x2160@60Hz	x
5	USB-C suporte até 5120x3200@60Hz	x
6	Thunderbolt suporte até 5120x3200@60Hz	x
7	14” FHD (1920 x 1080), IPS, Anti-Glare, Non-Touch, 100%sRGB, 400 nits, 60Hz, FHD IR/RGB Hybrid com Microphone, WWAN	x
Memória		
8	16GB (2x 8GB) DDR4-3200MHz SoDIMM	x
9	Capacidade de suporte até 64GB DDR4-3200 + 2 DDR4 SO-DIMM slots, com capacidade de dual-channel	x
Disco		
10	256 GB SSD M.2 2242 PCIe Gen4 TLC Opal (Capacidade de encritação incluida)	x
11	Capacidade de suporte até 1TB M.2 2242 SSD	x
Diversos		
13	NFC, Smart Card Reader, Fingerprint Reader, Wired Ethernet	x
14	3 Cell Li-Polymer 57Wh	x
15	Até 10.3 hr com 999 performance score @200nits JEITA 2.0 Até 14.9 hr @150nits Local video playback Até 16.1 hr @150nits	x
16	65W USB-C AC Adapter	x
17	Intel® Wi-Fi 6 AX201 2x2 AX vPro® & Bluetooth® 5.1 or above	x
Certificações		

18	EPEAT Gold ENERGY STAR 8.0 ErP Lot 3 TCO Certified RoHS compliant MIL-STD-810H military test passed	x
Interfaces		
19	Portas: >= 1x USB 3.2 Gen 1 >= 1x USB 3.2 Gen 1 (Always On) >= 1x USB-C 3.2 Gen 1 (support data transfer, Power Delivery 3.0 and DisplayPort 1.4) >= 1x Thunderbolt 4 / USB4 40Gbps (support data transfer, Power Delivery 3.0 and DisplayPort 1.4) >= 1x HDMI, up to 4K/60Hz >= 1x microSD card reader >= 1x Ethernet (RJ-45) >= 1x Headphone / microphone combo jack (3.5mm) >= 1 x Smart card reader	x
20	Deverá incluir docking station, que deverá ser suportada pelos endpints, com as seguintes capacidades: Refresh rate - 2x 3840x2160 @60 Hz; 1x 3840x2160 @30 Hz Power - 65 W with 90 W power adapter connected; 100 W with 135 W power adapter connected Compliance - FCC/ICES; CE; KCC; RCM; BSMI; VCCI; CB; cULus; EAC; TUV-Mark; Serbia Kvalitet; LoA; Israel SII; Ukraine DoC; NOM Interfaces: >= 1x Combo Audio Jack; >= 3x USB3.1; >= 2x USB2.0; >= 1x USB-C; >= 2x Display Port; >= 1x HDMI Port; >= 1x Gigabit Ethernet;	x
21	Deverá incluir 5 anos de garantia	x

- **Endpoint Avançado**

REQ	Requisito	Requisito Obrigatório
	Processador	
1	12th Generation Intel® Core™ i7-1265U Processor (E-cores up to 3.60 GHz P-cores up to 4.80 GHz) ou equivalente	x
Sistema Operativo		
2	Windows 11 Pro 64 Portuguese/English	x
Ecrã		
3	1080P FHD IR/RGB Hybrid with Microphone	x
4	Capacidade de suporte até 4 displays (display nativo e 3 displays externos via HDMI e Thunderbolt)	x
5	HDMI suporte até 4K@60Hz	x
6	Thunderbolt suporte até 5K@60Hz	x
7	13.3" WUXGA (1920 x 1200), IPS, Anti-Glare, Touch, 72%NTSC, 300 nits, LED Backlight, Low Cost Low Weight, FHD IR/RGB Hybrid com Microphone & Camera Cover of internal camera, Human Present Detection, 4G WWAN, PPS	x
Memória		
8	16 GB LPDDR5-6400MHz (Soldada)	x
Disco		
9	512 GB SSD M.2 2280 PCIe TLC Opal (Capacidade de encriptação incluída)	x
10	Capacidade de suporte até 2 TB M.2 2280 SSD	x
Diversos		
12	Ethernet - USB-C to RJ45	x
13	NFC, Smart Card Reader	x
14	4 Cell Li-Polymer 54.7Wh Suporte para Rapid Charge (carregamento até 80% em 1hr)	x
15	Até 11.3 hr com 982 performance score @200nits Até 9.7 hr com 791 performance score @250nits JEITA 2.0: Até 19.5 hr @150nits Local video playback Até 15.2 hr @150nits	x
16	65W USB-C AC Adapter	x
17	Intel® Wi-Fi 6E AX211 2x2 AX & Bluetooth® 5.2 or above with vPro®	x
Certificações		
18	EPEAT Gold EPEAT Gold ENERGY STAR 8.0 ErP Lot 3 TCO Certified 9.0 RoHS compliant MIL-STD-810H military test passed	x
19	Portas: >= 1 X Smart card reader	x

	>= 2x Thunderbolt 4 / USB4 40Gbps (support data transfer, Power Delivery 3.0 and DisplayPort 2.0) >= 1x USB 3.2 Gen 1 >= 1x USB 3.2 Gen 1 (Always On) >= 1x HDMI, up to 4K/60Hz >= 1x Headphone / microphone combo jack (3.5mm)	
20	Deverá incluir 5 anos de garantia	x

- **Display**

Abaixo encontram-se descritas as características dos displays a adquirir, sendo que deverão ser 100% compatíveis com os endpoints.

REQ	Requisito	Requisito Obrigatório
Características		
1	WLED	x
2	Capacidade de Suporte para Windows® 10, Windows 11	x
3	Diagonal Size – 23.8”	x
4	Interfaces – USB 3.2 Gen 1 / USB-C hub	x
5	Aspect Ratio – 16:9	x
6	Resolution - 2560x1440 300 nits	x
7	Refresh Rate – 60Hz	x
8	Contrast Ratio – 1000:1	x
9	>= 1x HDMI® 2.0, >=1x DP 1.4, >=1x DP Out, >=1x USB-C® 3.2 Gen 1 (DP 1.4 Alt Mode)	x
10	>= 4x USB 3.2 Gen 1 (1x BC 1.2), 1x USB-C® 3.2 Gen 1	x
11	>= 1x RJ45, Ethernet (10M/100M/1000M)	x
12	Deverá incluir 5 anos de garantia	x

- **Segurança de dispositivos**

Pretende-se adquirir uma ferramenta de monitorização e deteção de ameaças, vulnerabilidades e malware para ser utilizada na nossa infraestrutura para um total de 300 endpoints e/ou servidores. Abaixo encontram-se descritas as características da ferramenta a adquirir onde devem estar incluídas todas as licenças necessárias para as funcionalidades pretendidas, durante o período equivalente ao período de garantida, dos equipamentos a fornecer.

REQ	Requisito
1	Prevenção contra exploits, incluindo aqueles que utilizam vulnerabilidades do tipo Zero-Day.
2	Prevenção contra a execução de malware, sem requerer qualquer conhecimento prévio.
3	Garantir uma análise forense detalhada dos ataques prevenidos.
4	Capacidade de restringir a execução de determinados ficheiros.
5	Proteger contra ransomware.
6	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.
7	Controlar dispositivos USB
8	Disk Encryption
9	Host Firewall
10	Permitir isolar automaticamente da rede máquinas infetadas com malware
11	Módulo de Endpoint Detection and Response (EDR)
Gestão	
12	A solução proposta deve ser gerida através de uma interface gráfica web.
13	A solução proposta deve poder exportar os seus logs em formato syslog para qualquer solução de gestão de logs.
14	A solução proposta deve ter uma gestão centralizada baseada em cloud.
15	A solução deve vir de base já configurada com as best practices do fabricante de forma a simplificar o deployment da mesma.
16	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.
17	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.
18	A solução proposta deve suportar a atualização de software dos agentes de endpoint diretamente a partir da cloud.

Prevenção de Exploits	
19	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.
20	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.
21	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.
22	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.
23	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.
24	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.
25	A solução proposta deve proteger de forma simultânea todas as aplicações e processos do endpoint contra técnicas de exploit.
26	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.
27	A solução proposta deve conseguir proteger o endpoint contra “Kernel privilege escalation”.
28	A solução proposta deve também conseguir proteger contra exploits para MacOS e Linux como por exemplo “local privilege escalation”.
Prevenção de Malware	
29	A solução proposta deve suportar proteção contra a execução de executáveis maliciosos.
30	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.
31	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.

32	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.
33	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).
34	A solução proposta deve ser capaz de prevenir a execução de malware através da análise de comportamentos desencadeados pelo malware.
35	A solução proposta deve garantir a possibilidade de configurar whitelists globais para permitir a execução de certos ficheiros executáveis.
36	A solução proposta deve ser capaz de criar regras de exclusão das capacidades de protecção para endpoints específicos.
37	A solução proposta deve detectar e bloquear malware através do uso de machine learning e não deve utilizar assinaturas locais independentemente do sistema operativo
38	A solução deve ser capaz de analisar ficheiros do tipo mach-o, ELF e APK.
39	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.
40	A solução proposta deve conseguir perguntar aos serviços APT na cloud por valores de hash para verificar se determinado ficheiro é malicioso ou benigno.
41	A solução deve utilizar técnicas locais de machine learning para detetar malware desconhecido
42	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.
Requisitos	
43	A solução proposta deve ter a capacidade de submeter aos serviços APT na cloud ficheiros potencialmente maliciosos.
44	A solução proposta deve conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do malware.
45	A solução proposta não deve analisar ficheiros que já tenham sido anteriormente submetidos aos serviços APT na cloud.
46	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.
47	A solução proposta deve ter a capacidade de modificar manualmente a decisão tomada pelos serviços APT na cloud para uma hash em particular.
48	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.

49	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.
50	A solução proposta deve garantir a capacidade de efetuar análises estáticas (machine learning) em modo offline para Windows, Linux e macOS.
51	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.
52	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.
53	A solução proposta deve conseguir prevenir ataques que tirem partido do kernel para carregar e correr código "shell" malicioso.
54	A solução proposta deve conseguir que o módulo de análise de comportamentos de ransomware opere em modo de notificação ou de prevenção.
55	A solução proposta deve possuir um módulo de análise de comportamentos de ransomware que suporte os seguintes sistemas de ficheiros: NTFS, FAT, exFAT.
56	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.
57	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.
58	A solução deve suportar os seguintes sistemas operativos:
59	Android 5, 6, 7, 8, 9 e 10
60	Debian 8 e 9
61	CentOS 6 e 7
62	Oracle 6 e 7
63	Red Hat 6 e 7
64	SUSE 12
65	Ubuntu 12, 14, 16 e 18
66	macOS 10.11, 10.12, 10.13, 10.14 e 10.15
67	Windows 7, 8, 10 e 11
68	Windows Server 2008R2, 2012, 2016 e 2019
69	A solução deve suportar ainda os seguintes ambientes virtuais: Citrix XenApp, Citrix App layering, VMware AppVolumes, Vmware ThinApp
Endpoint Detection and Response	
70	Capacidade de 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.

71	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.
72	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.
73	Quando diferentes alertas estão relacionados, a solução deve ser capaz de os agregar automaticamente em um único incidente.
74	Deve ser possível agregar diferentes incidentes num único.
75	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.
76	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.
77	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)
78	A solução deve mapear os diferentes alertas para a Framework Mitre ATT&CK
79	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.
80	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.
81	Deve existir uma funcionalidade de “search&destroy” que permite pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo
82	A solução deve aprender o comportamento de cada máquina e criar perfis de forma a ser capaz de identificar comportamentos anômalos
83	Com base na aprendizagem comportamental para cada máquina e utilizador a solução deverá ser capaz de gerar alarmística para estes cenários:
84	Sessão rara de SSH
85	Uso de comandos fora do comum (arp -a, ipconfig, etc)
86	processos raros a comunicar com máquinas fora da organização

87	processos a comunicar com máquinas externas que não são normalmente acedidas pelas máquinas da organização
88	scripts a comunicar com hosts externos
89	listagem de utilizadores do domínio
90	comando de powershell anormal
91	volume de conexões entre máquinas elevado
92	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.
Visibilidade sobre as máquinas	
93	A solução deve incluir, através de licenciamento adicional, um módulo de visibilidade com as seguintes características:
94	Capacidade de identificar:
95	Utilizadores e grupos configurados em cada máquina
96	Serviços a correr nas máquinas
97	Drivers instalados nas máquinas
98	Processos, drivers, serviços que são automaticamente inicializados sempre que o utilizador liga as máquinas.
99	Shares de rede configurados nas máquinas
100	Discos existentes nas máquinas
101	Funcionalidade de "search&destroy" que permita pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo
102	Identificar vulnerabilidades e respetiva criticidade para ambientes Windows e Linux
103	Identificar as aplicações a correr em cada equipamento
Resposta a Incidentes	
104	A solução proposta deve permitir iniciar scans de malware à máquina infetada
105	Deve ser possível efetuar blacklist e whitelists a hashes
106	Deve ser possível fazer quarentena a determinados processos
107	Durante a investigação de um incidente, a solução deve permitir isolar da rede máquinas infetadas
108	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.
109	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.
110	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.
111	Capacidade de criar regras de correlação personalizadas que permitem detectar ataques retroativamente.
112	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.
113	Deverá incluir licenciamento para as funcionalidades pretendidas durante um período de 5 anos

1. Serviços de implementação, tem de estar incluídos no fornecimento do software de endpoint security, os serviços de instalação e configuração do software nos equipamentos.
2. O concorrente obriga-se a constituir uma equipa técnica com as competências necessárias ao bom desempenho dos trabalhos de implementação e de acordo boas práticas da área, isto é, com a competências necessárias à instalação e configuração da componente de segurança.

   Deverá ainda ser acompanhada por um gestor de projeto com os seguintes objetivos:
   - Acompanhamento e reporte diário à equipa do IAVE, de eventuais desvios do plano de intervenção estipulado e seus motivos;
   - Reporte à equipa do IAVE de deteção de possíveis avarias nos equipamentos novos no ato da instalação para efeito de registo de garantia dos mesmos.
   - Intervir sobre qualquer dúvida que possa surgir à equipa de terreno, no âmbito do serviço prestado.
   - Gestão diária dos relatórios de aceitação, devidamente validados pelo responsável do Local/Site.

   Os serviços a desenvolver abrangem as seguintes atividades:
   - Elaboração de planos de:
     - Implementação/migração
     - Testes e relatórios de serviço
     - Riscos
   - Documentação de projeto
   - Passagem de conhecimento