CADERNO DE ENCARGOS

CONCURSO PÚBLICO

Procedimento n.º 61/2020/IGeFE

Aquisição de plataforma de *software* de monitorização e correlação de eventos - SIEM

(NOS TERMOS DA ALÍNEA B) DO N.º 1 DO ARTIGO 20.º E DO ARTIGO 130.º E SEGUINTES DO CÓDIGO DOS CONTRATOS PÚBLICOS, NA SUA ATUAL REDAÇÃO)

Instituto de Gestão Financeira da Educação, I.P.
Núcleo de Contratação Pública
Departamento de Administração Geral e Contratação Pública

Parte I

Cláusulas Jurídicas

Cláusula 1.ª
Objeto

1. O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar pelo Instituto de Gestão Financeira da Educação, I.P. (doravante também designado por IGeFE, I.P.), na sequência do procedimento pré-contratual por concurso público que tem por objeto a «Aquisição de plataforma de *software* de monitorização e correlação de eventos - SIEM», nos termos da alínea b) do n.º 1 do artigo 20.º e do artigo 130.º e seguintes do Código dos Contratos Públicos, aprovado em anexo ao Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua atual redação, doravante também designado por CCP.
2. A descrição das especificações técnicas relativas à plataforma de *software* a adquirir, bem como os serviços inerentes à sua aquisição, é a que se encontra definida na Parte II do presente caderno de encargos.
3. Os serviços de instalação, formação, customização, suporte e manutenção da plataforma, nomeadamente, relativamente a novos *updates* e *upgrades* de versão, bem como a correção de *bugs* existentes no software a adquirir no âmbito do presente procedimento, serão assegurados por um período de 3 (três) anos, sendo o valor pago integralmente com a aquisição referida no n.º 1 da presente cláusula.
4. O presente procedimento insere-se no CPV 48730000-4: Pacote de software de segurança a que se refere o Regulamento (CE) n.º 213/2008 da Comissão, de 28 de Novembro de 2007, publicado no Jornal Oficial da União Europeia, L 74.

Cláusula 2.ª
Forma e documentos contratuais

1. O contrato é composto pelo presente clausulado contratual e seus anexos.
2. O contrato a celebrar integra os seguintes elementos:
   a) Os suprimentos dos erros e das omissões do Caderno de Encargos identificados pelo concorrente, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
   b) Os esclarecimentos e as rectificações relativos ao Caderno de Encargos;
   c) O Caderno de Encargos;
   d) A proposta adjudicada; e
   e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem pela qual são indicados nesse número.

4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e respetivos anexos, prevalecem os primeiros, salvo quanto aos ajustamentos ao conteúdo do contrato propostos de acordo com o disposto no artigo 99.º do CCP e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma.

Cláusula 3.ª

Entidade Adjudicante

A entidade adjudicante é o Estado Português através do Instituto de Gestão Financeira da Educação, I.P. com sede na Avenida 24 de Julho, n.º 134, 5.º piso, em Lisboa.

Cláusula 4.ª

Preço base e preço contratual

1. O preço base fixado nos termos e para os efeitos previstos no n.º 1 do artigo 47.º do CCP, é o preço máximo a que a Entidade Adjudicante se dispõe pagar pela aquisição de uma plataforma de software de monitorização e correlação de eventos - SIEM, bem como pelos serviços de instalação, formação, customização, suporte e manutenção à mesma, que constituem o objeto do presente procedimento, sendo definido em € 74.500,00 (setenta e quatro mil e quinhentos euros), valor ao qual acresce o IVA à taxa legal em vigor.

2. O preço contratual é o preço constante da proposta adjudicada pela entidade adjudicante, acrescido de IVA à taxa legal em vigor.

3. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não estejam expressamente atribuídas à entidade adjudicante.

Cláusula 5.ª

Condições de pagamento

1. A entidade adjudicante obriga-se a pagar ao adjudicatário o valor correspondente à aquisição do bem objeto do presente procedimento, bem como aos serviços de instalação, formação, customização, suporte e manutenção constantes da proposta adjudicada, acrescido de IVA à taxa legal em vigor.
2. O preço identificado no número anterior é o que resultar do disposto neste caderno de encargos e da proposta apresentada, não podendo em caso algum ser superior ao preço base definido na Cláusula 4.ª.
3. Os pagamentos são efetuados no prazo máximo de 60 (sessenta) dias, após a entrega das respetivas faturas, nos termos dos artigos 299.º, 299.º-A e 326.º do CCP.
4. Em caso de discordância por parte da entidade adjudicante, quanto aos valores indicados nas faturas, este deve comunicar ao adjudicatário, por escrito, os respetivos motivos, ficando o

adjudicatário obrigado a prestar os esclarecimentos necessários e/ou a proceder à emissão de nova fatura corrigida.

5. Em caso de atraso no cumprimento das obrigações pecuniárias pela entidade adjudicante, é aplicável o disposto nos artigos 299.º, 299.º-A e 326.º do CCP.

6. Não há lugar à revisão ou à atualização do preço contratual.

7. Desde que devidamente emitidas e observado o disposto nos números anteriores, as faturas são pagas por transferência bancária para conta a indicar pelo adjudicatário.

8. As faturas devem indicar, sob pena de nulidade, o número de compromisso que será indicado pela entidade adjudicante.

9. O atraso, em qualquer momento, por parte da entidade adjudicante no cumprimento de obrigações pecuniárias não autoriza o adjudicatário a invocar a exceção de não cumprimento de quaisquer obrigações previstas no contrato celebrado, salvo se a invocação da exceção de não cumprimento não implicar grave prejuízo para a realização do interesse público.

Cláusula 6.ª

Obrigações do adjudicatário

1. O adjudicatário obriga-se a executar o objeto do contrato de forma profissional e competente, utilizando os conhecimentos técnicos, o *know-how*, a diligência, o zelo e a pontualidade próprios das melhores práticas.

2. Constituem ainda obrigações do adjudicatário:

   a) Apresentar os documentos de habilitação a que está obrigado, nos termos do artigo 81.º do CCP;

   b) Disponibilizar a plataforma de *software* de monitorização e correlação de eventos – SIEM;

   c) Assegurar os serviços de instalação, formação, customização, suporte e manutenção à plataforma identificada na alínea anterior junto da entidade adjudicante, conforme as condições definidas no presente caderno de encargos e demais documentos contratuais;

   d) Garantir junto da entidade adjudicante, o funcionamento eficaz da plataforma, durante o período previsto no n.º 2 da cláusula 1.ª do presente caderno de encargos;

   e) Recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução do contrato;

   f) Dar cumprimento, a todo o momento, às obrigações legais relativas aos serviços prestados, assegurando a execução dos mesmos de acordo com as melhores regras técnicas e de arte conhecidas e praticadas;

   g) Analisar e levar em consideração todas as situações e circunstâncias relevantes para a execução do contrato, incluindo, entre outras e a título meramente exemplificativo, a

informação prévia necessária, as circunstâncias de modo, tempo e lugar e os meios de modo a salvaguardar que os serviços serão prestados nos termos contratados, sem hiatos, falhas ou interrupções que pudessem ter sido previstas;

h) Assumir todos os riscos inerentes à prestação dos serviços, bem como aqueles que, em concreto, apenas sejam ou possam ser do conhecimento do adjudicatário ou por este gerido em primeira linha;

i) Garantir, a todo o momento, a correta, completa e adequada articulação e compatibilização entre os serviços prestados e a finalidade a que os mesmos se dirigem com outros serviços ou outras finalidades que com eles estejam ou possam estar em relação, de modo a não afetar negativamente quaisquer outros serviços, produtos ou soluções dos contraentes públicos, assumindo, em cada momento, o respetivo risco de interface;

j) Comunicar antecipadamente, logo que tenha conhecimento, à entidade adjudicante, o facto que torne parcial ou totalmente impossível a prestação do serviço objeto do procedimento, ou o cumprimento de qualquer outra das suas obrigações nos termos do contrato a celebrar com a entidade adjudicante;

k) Não subcontratar, no todo ou em parte, a execução do objeto do contrato, sem prévia autorização escrita concedida pela entidade adjudicante;

l) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenha no âmbito da formação e execução do contrato, nem utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, trabalhadores, colaboradores ou terceiros que nela se encontrem envolvidos;

m) Prestar de forma correta, atempada e fidedigna as informações referentes às condições em que são prestados os serviços de instalação, formação, customização, suporte e manutenção à plataforma, bem como prestar, por escrito ou de forma oral, ao contraente público, todos os esclarecimentos que se justifiquem ou que este entenda necessários;

n) Executar a prestação dos serviços de instalação, formação, customização, suporte e manutenção à plataforma, disponibilizando sempre aquela que seja, em cada momento e no respeito pelo objeto contratado, a solução mais recente, completa e funcional, obrigando-se a informar imediatamente o contraente público caso venham a ocorrer atualizações ou novas funcionalidades inerentes aos serviços ora contratados;

o) Comunicar qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação e sede social, os seus representantes legais, a sua situação jurídica ou a sua situação comercial, bem como alterações dos seus quadros ou funcionários com relevância para a prestação de serviços;

p) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato.

Cláusula 7.ª

Obrigações da entidade adjudicante

Constituem obrigações da entidade adjudicante:

a) Pela disponibilização da plataforma e pelos serviços de instalação, formação, customização, suporte e manutenção abrangidos pelo presente procedimento, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, o IGeFE, I.P. deve pagar ao adjudicatário o preço constante da proposta adjudicada, acrescido do IVA à taxa legal em vigor;

b) Nomear um gestor do contrato, de acordo com o previsto no artigo 96.º e artigo 290.º-A, ambos do CCP e comunicar quaisquer alterações dessa nomeação;

c) Comunicar, em tempo útil, ao adjudicatário, os aspetos relevantes que tenham impacto no cumprimento do contrato.

Cláusula 8.ª

Prazo

1. O fornecimento da plataforma de *software* de monitorização e correlação de eventos – SIEM, bem como a sua instalação, configuração e integração na infraestrutura da entidade adjudicante, deverá estar integralmente concluídos até ao limite máximo do dia 31 de dezembro de 2020.
2. Os serviços de suporte e manutenção inerentes ao fornecimento da plataforma melhor identificada na cláusula 1.ª do presente caderno de encargos, nomeadamente, os relativos a novos *updates* e *upgrades* de versão, bem como a correção de *bugs* existentes no produto, serão assegurados durante 36 (trinta e seis) meses, contados a partir da data em que a plataforma SIEM for disponibilizada à entidade adjudicante.

Cláusula 9.ª

Direitos de propriedade intelectual e industrial

1. O adjudicatário deve ser titular de todas as licenças, autorizações ou demais atos de consentimento legalmente necessários à utilização de *software* e demais soluções ou produtos por si utilizados na execução do contrato, sendo da sua inteira responsabilidade qualquer encargo decorrente da utilização indevida dos mesmos.
2. Sempre que legalmente admissível e na máxima extensão admitida na Lei, o resultado da prestação dos serviços é propriedade da entidade adjudicante.

Cláusula 10.ª

Sigilo e confidencialidade

1. O adjudicatário obriga-se a guardar sigilo e confidencialidade sobre toda a informação e documentação, técnica e não técnica, comercial, financeira, organizativa, laboral ou outra, relativamente à entidade adjudicante, a que tenham acesso ao abrigo ou em relação com a execução do contrato, independentemente do suporte da mesma (escrito, verbal ou suporte informático), sendo esta obrigação extensível aos seus agentes, funcionários, colaboradores ou terceiros que as mesmas envolvam.
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, salvo se tal for autorizado expressamente, por escrito, pela entidade adjudicante.
3. O adjudicatário é responsável pelo cumprimento do dever de sigilo por parte dos seus trabalhadores ou colaboradores, qualquer que seja a natureza jurídica do vínculo que sirva de base a essa colaboração, inclusivamente após a cessação desta, independentemente da causa da cessação, devendo informá-los da respetiva natureza confidencial e adotar todas as medidas que se mostrem necessárias para salvaguardar essa confidencialidade.
4. O adjudicatário é ainda responsável perante o IGeFE, I.P., em caso de violação do dever de sigilo pelos terceiros por si subcontratados, bem como por quaisquer colaboradores desses terceiros.
5. O adjudicatário deve devolver ou destruir, conforme solicitado pela entidade adjudicante, toda a informação a que tenha tido acesso no âmbito do procedimento pré-contratual e do contrato e que se encontre abrangida pela presente cláusula, logo que a mesma deixe de ser necessária ao cumprimento das suas obrigações, a solicitação da entidade adjudicante ou com a cessação do contrato por qualquer motivo.
6. Exclui-se do dever de sigilo previsto a informação e a documentação que sejam comprovadamente do domínio público, à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 11.ª

Responsabilidade

1. O adjudicatário assume a responsabilidade, por si e pelos técnicos seus colaboradores, pela perfeita adequação dos trabalhos que realizar e das condições neles previstos à realidade e particularidades dos fins a que se destinam.
2. O adjudicatário é responsável por todos os atos e omissões dos quais possam resultar prejuízos para a entidade adjudicante ou para terceiros, incluindo os praticados através da ação dos seus

funcionários, ainda que tais atos ou omissões sejam dolosa ou negligentemente praticados contra ordens ou instruções que aquele lhes haja transmitido, no âmbito dos poderes de autoridade e direção que sobre os mesmos exerce.

3. O adjudicatário é responsável perante a entidade adjudicante por qualquer indemnização que esta tenha de pagar a terceiros e por quaisquer pedidos, processos, danos, custos, perdas e despesas em que a entidade adjudicante incorra, na medida em que tal resulte de negligência, incumprimento ou cumprimento defeituoso por parte do adjudicatário de qualquer das obrigações assumidas na proposta que apresentou para a celebração do contrato em causa.

4. Se a entidade adjudicante tiver de indemnizar terceiros, ou proceder ao pagamento de custos ou despesas de qualquer natureza, com fundamento na violação de obrigações do adjudicatário, gozará de direito de regresso contra este último por todas as quantias despendidas, incluindo as despesas e honorários dos mandatários forenses.

Cláusula 12.ª

Resolução por iniciativa da entidade adjudicante

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na Lei, designadamente, por motivos de interesse público, o IGeFE, I.P. pode resolver o contrato celebrado, a título sancionatório, no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem no âmbito do contrato, designadamente, nos seguintes casos:

    a) Se o adjudicatário se encontrar em qualquer das situações previstas no artigo 55.º do Código dos Contratos Públicos;

    b) Se o adjudicatário não entregar atempadamente a documentação que lhe venha a ser solicitada pela entidade adjudicante;

    c) Se o adjudicatário prestar falsas declarações no âmbito da execução do contrato;

    d) Recusa de prestação de serviços à entidade adjudicante.

2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao adjudicatário e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pelo IGeFE, I.P.

3. Em caso de incumprimento pelo adjudicatário, que conduza à resolução do contrato, o adjudicatório constitui-se na obrigação de indemnizar a entidade adjudicante nos termos gerais de direito.

Cláusula 13.ª

Resolução do contrato por iniciativa da entidade adjudicatária

1. Os fundamentos de resolução são os previstos na Lei e no Código dos Contratos Públicos.

2. O adjudicatário pode resolver o contrato em caso de atraso, por parte da entidade adjudicante,

superior a 60 (sessenta) dias, no pagamento de faturas que se mostrem devidas e se o montante em dívida exceder 25 % do preço contratual, excluindo juros.

3. Nos casos previstos no n.º 1 e 2, o direito de resolução pode ser exercido mediante declaração enviada ao IGeFE, I.P., a qual produz efeitos 30 (trinta) dias após a data de 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 da presente cláusula não determina a cessação das obrigações do adjudicatário relativamente aos serviços já prestados.

Cláusula 14.ª

Cessão da posição contratual e subcontratação

1. O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato, nem subcontratar, sem autorização prévia e por escrito do IGeFE, I.P.
2. Para efeitos das autorizações previstas no número anterior, deve, sem prejuízo do que também for legalmente devido:
    a) Ser apresentada pelo cessionário ou subcontratado, toda a documentação exigida ao adjudicatário no presente procedimento;
    b) O IGeFE, I.P. deve apreciar, designadamente, se o cessionário ou subcontratado, não se encontra em nenhuma das situações previstas no artigo 55.º do CCP, e se tem capacidade técnica e financeira para assegurar o exato e pontual cumprimento do contrato.

Cláusula 15.ª

Casos fortuitos ou de força maior

1. Não podem ser impostas penalidades ao adjudicatário, 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.

2. Podem constituir força maior, os requisitos do número anterior, se se verificarem 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) Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
b) Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;
d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;
e) Incêndios ou inundações com origem nas instalações do adjudicatário 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 do adjudicatário não devidas a sabotagem;
g) Eventos que estejam ou devam estar cobertos por seguros.

4. O adjudicatário é responsável pelos atos e omissões que possam causar prejuízos à entidade adjudicante ou a terceiros, praticados através da ação dos seus trabalhadores, colaboradores e subcontratados, ainda que tais atos ou omissões sejam dolosa ou negligentemente praticados em violação de ordens ou instruções que aquela lhes haja transmitido, no âmbito dos poderes de autoridade e direção que exerce sobre os mesmos.

5. A ocorrência de circunstâncias que possam consubstanciar casos fortuitos ou de força maior deve ser imediatamente comunicada e justificada à outra parte, devendo quem a invocou informar igualmente do prazo previsível para o restabelecimento da situação.

6. 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 16.ª

Encargos do adjudicatário

1. Todas as despesas ou encargos em que o adjudicatário incorra para o cumprimento das obrigações emergentes do contrato são da sua exclusiva responsabilidade e não podem ser reclamados à entidade adjudicante, a menos que outro regime decorra da Lei ou do contrato.

2. São, designadamente, da responsabilidade do adjudicatário:

a) Quaisquer impostos, taxas, direitos de qualquer natureza ou outros encargos exigidos pelas autoridades competentes e relativos à celebração e execução do contrato em Portugal ou nos territórios do país ou países do adjudicatário ou de passagem em transporte;

b) Encargos com a obtenção de autorizações, licenças, aprovações que, nos termos da Lei e regulamentação, lhe sejam aplicáveis e/ou se mostrem necessárias para o cumprimento das obrigações decorrentes do contrato, bem como o pagamento de quaisquer emolumentos exigidos pelas autoridades competentes relativamente ao cumprimento das obrigações contratuais do adjudicatário;

c) Encargos decorrentes da utilização, na execução do contrato, de marcas registadas, de patentes registadas ou de licenças, designadamente, de utilização de *software*, ou outros elementos protegidos por direitos de propriedade intelectual, bem como a obtenção das respetivas autorizações necessárias;

d) Despesas respeitantes ao cumprimento da obrigação de prestação de quaisquer garantias exigidas no contrato, designadamente, de bom e pontual cumprimento.

Cláusula 17.ª

Dever de Informação

1. O adjudicatário obriga-se a prestar a informação e esclarecimentos que lhe forem solicitados pela entidade adjudicante, com a periodicidade que este razoavelmente entender conveniente, quanto à execução dos serviços e ao cumprimento das obrigações que para aquele emergirem do contrato.

2. O adjudicatário obriga-se a comunicar de imediato, no prazo de 10 (dez) dias, à entidade adjudicante o início ou a iminência de qualquer processo judicial ou extrajudicial que possa conduzir à sua declaração de insolvência, a providência análoga à insolvência ou à sua extinção, bem como a verificação de qualquer outra circunstância que perturbe a execução do contrato.

Cláusula 18.ª

Sanções

1. O incumprimento das obrigações do adjudicatário determina a aplicação de sanções pecuniárias por parte da entidade adjudicante, até 5% do valor da adjudicação.
2. O valor das sanções constantes do número anterior é descontado na fatura relativa ao período em que se deu o facto que originou a sua aplicação.
3. As penas pecuniárias previstas na presente cláusula não obstam a que a entidade adjudicante exija uma indemnização pelo dano excedente.

Cláusula 19.ª

Resolução sancionatória por incumprimento contratual

1. O incumprimento contratual definitivo confere à entidade adjudicante o direito à resolução do contrato.

2. A resolução do contrato não prejudica a aplicação de quaisquer sanções pecuniárias, nos termos da cláusula anterior.

Cláusula 20.ª

Comunicações e notificações

1. Em sede de execução contratual, todas as comunicações ou notificações da entidade adjudicante dirigidas ao adjudicatário são efetuadas por escrito e enviadas através de correio eletrónico com aviso de entrega, carta registada com aviso de receção ou fax, de acordo com os seguintes elementos:

   Morada: Av. 24 de Julho, n.º 134 – 5.º - 1399-029 Lisboa

   Fax: 213907003

   e-mail: compras@igefe.mec.pt

   Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

2. As comunicações entre a entidade adjudicante e o adjudicatário devem ser redigidas em português, podendo ser efetuadas através de correio eletrónico ou de outro meio de transmissão escrita e eletrónica de dados, ou por via postal, por meio de carta registada ou de carta registada com aviso de receção.

3. As notificações e as comunicações consideram-se feitas:

   a) Na data da respetiva expedição, quando efetuadas através de correio eletrónico ou de outro meio de transmissão escrita e eletrónica de dados, salvo o disposto no número seguinte;

   b) Na data constante do relatório de transmissão bem-sucedido, quando efetuado através de telecópia, salvo o disposto no número seguinte;

   c) Na data indicada pelos serviços postais, quando efetuadas por carta registada;

   d) Na data da assinatura do aviso, quando efetuadas por carta registada com aviso de receção.

Cláusula 21.ª

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.

Cláusula 22.ª

Resolução de Litígios

Para o conhecimento de quaisquer litígios emergentes do contrato, designadamente, os relativos à sua interpretação, execução, incumprimento, validade, resolução ou redução, é competente o foro da Comarca de Lisboa.

Cláusula 23.ª

Direito aplicável

Em tudo o que não for especificado no presente caderno de encargos, aplicam-se as disposições constantes no CCP, aprovado em anexo ao Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua atual redação, bem como as restantes disposições regulamentares em vigor, de acordo com a natureza do objeto a contratar.

Parte II
Especificações técnicas

Cláusula 24.ª
Requisitos gerais

1. A aquisição de uma plataforma de *software* de monitorização e correlação de eventos - SIEM, objeto do presente procedimento, deverá garantir o cumprimento dos requisitos técnicos constantes nos números seguintes.
2. O concorrente deve possuir certificações, **válidas à data da apresentação da proposta**, de, pelo menos, os seguintes fabricantes e no mínimo com os seguintes estatutos:
    2.1. Check Point – 3 Star Partner
    2.2. Cisco – Select Certified Partner
    2.3. Trend Micro – GOLD Partner
    2.4. Microsoft – GOLD Partner
    2.5. F5 Networks – Silver Partner.
3. O concorrente deve possuir, também a **acreditação de segurança**, **válida à data da apresentação da proposta**, com o grau **SECRETO**, certificando a sua idoneidade e confiabilidade para aceder, manusear, deter e guardar informação classificada para a marca NACIONAL com o grau SECRETO.
4. O concorrente deve integrar uma rede de CSIRT, nomeadamente, a Rede Nacional de CSIRT que coordena a resposta a incidentes em entidades públicas, operadores de serviços essenciais e de infraestruturas críticas nacionais e prestadores de serviços digitais.
5. A solução a fornecer deverá ser de um único fabricante, baseada na infraestrutura virtual existente no IGeFE, I.P., mais concretamente, ser compatível com estruturas de virtualização VMWare. A arquitetura visa disponibilizar à entidade adjudicante uma ferramenta com vista a sintetizar as seguintes funcionalidades base:
    5.1. Armazenamento e correlação de logs/traps;
    5.2. Monitorização e alarmística da infraestrutura dos centros de dados;
    5.3. Automatização de processos controlo e reação a eventos;
    5.4. Capacidade de segregação de ambientes “multi-tenant”;
6. A solução deve suportar o mínimo de 3000 EPS (eventos por segundo) com todas as componentes e funcionalidades ativas que assegurem a recolha, armazenamento, tratamento e análise de todos os registos (logs, traps, etc).
7. A solução apresentada **deve incluir o licenciamento** necessário que permita a implementação dos seguintes requisitos e tipologia:
    7.1. Gerir e monitorizar no mínimo de 250 dispositivos de rede e segurança;
    7.2. Gerir e monitorizar no mínimo de 50 servidores e aplicações (agentes específicos);
    7.3. Processar no mínimo 3000 EPS (eventos por segundo);

7.4. Processar no mínimo 100 indicadores de compromisso IOC;
7.5. Topologia multi-tenant (no mínimo 10 entidades);
7.6. Unificar numa única consola funções de NOC e SOC “Analytics”;
7.7. Disponibilizar uma CMDB nativa e sem recurso a módulos adicionais, com:
7.7.1. Rastreamento de hardware e software;
7.7.2. Análise de performance dos equipamentos;
7.7.3. Monitorização de equipamentos de rede, switch, firewalls, etc..;
7.8. Possibilidade de implementação de solução distribuída para corelação de eventos;
7.9. Possibilidade de customização “scripts” para correlação de eventos “parsing”;
7.10. Disponibilizar relatórios do tipo:
7.10.1. Compliance (PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13 and SANS);
7.10.2. Funcionais (Security, Availability, Performance);
7.10.3. Dispositivos e pedidos (ticket).

8. Com vista a possibilidade de escalar e melhorar o desempenho da solução face ao potencial crescimento do tráfego, a arquitetura da solução deverá permitir a instalação a qualquer momento de pelo menos 10 (dez) coletores (em software/VM) distribuídos pela infraestrutura da entidade adjudicante ou dos seus organismos/parceiros, sem quaisquer custos adicionais de licenciamento.
9. Entendimento das funções de **Coletor** – o coletor tem como função servir de interface, ponto de entrada, para os vários logs, e envia-los para a consola central onde vão ser processados e armazenados os logs.
10. A solução proposta deverá ter a capacidade de monitorizar e integrar eventos relativos aos seguintes tipos de equipamentos/plataformas existentes na infraestrutura:
10.1. Firewalls com IPS, Application Control, AV e Anti-bot (Check Point);
10.2. Proxy (Trend Micro);
10.3. Servidores de DNS;
10.4. Balanceadores de carga e WAF (F5 Networks);
10.5. Mail Relays (Trend Micro);
10.6. Gestores de DHCP e IPAM (Microsoft e linux);
10.7. Controladoras e APs Wi-Fi (p. ex. Cisco e HPE);
10.8. Switches de CORE (Cisco e HPE);
10.9. Consola centralizada de antivírus (Trend Micro);
10.10. Servidores de bases de dados (Microsoft SQL);
10.11. Controladores de Domínio (Microsoft Active Directory);
10.12. Websites (Microsoft IIS e Apache);
10.13. Servidores de correio eletrónico (Microsoft Exchange);
10.14. Servidores Microsoft SharePoint;
10.15. Hipervisores VMWare, Hiper-V e OVM (servidores e VDI);

10.16. Solução de backups (Commvault e Veeam);

10.17. Aplicações diversas (p.ex. SmartDOCs, Oracle).

11. Para fazer face a evoluções da infraestrutura, a solução deverá ter a possibilidade de integrar a monitorização, normalização e correlação de eventos provenientes de outros equipamentos, serviços e aplicações relevantes neste contexto que a entidade adjudicante venha a adquirir, através do desenho de novos parsers específicos e customizados.
12. Com o objetivo de uma eficiente e rápida resposta a incidentes, a solução deverá disponibilizar um sistema incorporado de *ticketing* e ter a capacidade para integrar de forma automatizada com outros sistemas de *ticketing* a disponibilizar e/ou correio eletrónico.

Cláusula 25.ª

Funcionalidades e capacidade da solução

Com vista à melhor qualidade e fiabilidade da informação e das análises, a solução proposta deverá ter as seguintes funcionalidades e capacidades:

1. Recolher métricas de monitorização de disponibilidade e desempenho de sistemas, aplicações, hipervisores (guest, host, resource pool e cluster level), bases de dados, armazenamento, redes e infraestruturas de comunicações, etc.;
2. Coletar informação de contexto dos equipamentos a serem monitorizados, cujos resultados deverão poder ser utilizados para o cálculo do rating da disponibilidade de serviço, através de:
   2.1. Descoberta ativa de equipamentos na rede, sem recurso a um agente, utilizando protocolos standard como: SNMP, WMI, VM SDK, OPSEC, JDBC, Telnet, SSH e JMX;
   2.2. Dados de estado e prontidão de serviços como DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH e Web em HTTP e HTTPS (Single and Multi-Step);
3. As métricas de desempenho recolhidas deverão incluir pelo menos as seguintes informações: utilização das interfaces, erros, bytes enviados e recebidos, CPU, memória, disco e utilização dos processos;
4. Possuir CMDB própria, interna e nativa da solução;
5. Descobrir, mapear e registar na CMDB interna, os dispositivos e aplicações encontrados, independentemente de terem existência física, virtualizada ou na cloud;
6. Armazenar na CMDB interna os resultados de contexto, com pelo menos a seguinte informação: Versão/Firmware/Sistema operativo instalado no equipamento, serial number do equipamento, interfaces configuradas, nome das interfaces, IP e subnet, estado das interfaces (enabled, disabled), security levels configurados, velocidade da interface, processos a correr nos equipamentos ou S.O.;
7. Produzir e enviar alertas sempre que ocorra uma alteração do estado de um processo a decorrer;
8. A informação dos equipamentos deverá ser populada na CMDB interna por grupos (por

exemplo: Windows Server Groups, Firewall Group, etc.);

9. As aplicações a correr (nos equipamentos) devem ser automaticamente identificadas e a CMDB interna populada por grupos aplicacionais, associando todos os equipamentos que correm essas aplicações (por exemplo: o grupo aplicacional “a correr o Microsoft IIS”);
10. Mapeamento automatizado de serviços de negócios por aplicação, infraestrutura ou grupo de equipamentos, com deteção de alterações de serviços de negócios, priorização, análise da resolução e impacto;
11. Possuir um modelo interno que defina automaticamente as métricas a serem coletadas para os dispositivos e os intervalos de coleta, quando a descoberta ativa dos equipamentos estiver concluída;
12. Construir padrões de utilização e detetar desvios de desempenho;
13. Detetar alterações, registar e fornecer comparações de configurações na rede em tempo-real;
14. Agregar dados de forma unificada e holística de logs, métricas de desempenho da rede, traps SNMP, alertas de segurança e alterações de configurações;
15. Fornecer uma interface de análise unificada que permita, com uma única linguagem de consulta, analisar dados de log (eventos) e dados de desempenho;
16. Identificar e associar dinamicamente utilizadores aos respetivos endereços IP, MAC Address e localização geográfica;
17. Executar scripts ou outras ações baseadas em triggers sobre eventos e incidentes, com vista a reagir de forma automatizada a ameaças, como por exemplo desabilitar contas de utilizadores, portas de rede, bloquear endereços de IP em firewalls ou desassociar utilizadores de redes wireless;
18. Integrar e correlacionar fontes de informação (feeds) relativos a ameaças (Threat Intelligence) e indicadores de comprometimento (IoC) de origem comercial ou de acesso aberto, contendo domínios maliciosos, reputação de IPs, hashes, etc.;
19. Permitir a integração de informação (feeds) através de ficheiros CSV executada via GUI;
20. Permitir correlacionar informação proveniente de feeds com eventos do SIEM em tempo real e de feeds com eventos do histórico do SIEM;
21. Realizar a recolha, parsing, normalização, indexação e armazenamento dos eventos de segurança sem impacto no ambiente de produção;
22. Disponibilizar agentes para recolha de informação relativa a monitorização de integridade de ficheiros, software instalado e alterações ao nível do registry de servidores para sistemas Windows e Linux;
23. Os agentes Windows fornecidos pelo SIEM, que deverão ser geridos centralmente, deverão proporcionar pelo menos as seguintes caraterísticas:
    - 23.1. Coletar logs de arquivos de texto em dispositivos Windows;
    - 23.2. Coletar logs de eventos para além de segurança, sistema e aplicativos;
    - 23.3. Monitorizar a integridade de ficheiros;

23.4. Monitorizar a integridade e atividade do registry;
23.5. Monitorizar dispositivos removíveis;
23.6. Executar comandos PowerShell e enviar os outputs como logs;
23.7. Enviar os dados dos eventos para o SIEM de forma encriptada (HTTPS);

24. Categorizar e associar fluxos de informação e/ou componentes da infraestrutura a áreas organizacionais para relatórios por áreas, serviços e aplicações;
25. Construir padrões de comportamento de dispositivos, utilizadores e servidores, definindo alertas automáticos para desvios registados;
26. Proporcionar um sistema de alertas e notificações automáticas baseado em políticas;
27. Armazenar "event logs" em formato "raw";
28. A informação dos eventos deverá ser armazenada de forma comprimida e sem recurso uma base de dados relacional;
29. O arquivo de logs deverá ser feito com hashing para garantia de integridade;
30. O processamento de dados de eventos deve ser executado por parsers no sistema que deverão poder ser modificados e personalizados através da GUI sem necessidade de acesso ao CLI;
31. Possuir a capacidade de adicionar novos atributos/variáveis para análise, dispositivos e tipos de eventos através da GUI sem necessidade de acesso ao CLI;
32. Permitir acesso baseado em regras (RBAC) para restringir o acesso aos dados e GUI da solução;
33. Suportar a autenticação externa através pelo menos de Active Directory, LDAP e Radius;
34. Capacidade de exportar e importar *dashboards*, relatórios e regras via XML;
35. Disponibilizar a informação em modo de "*dashboards*"
36. Disponibilizar gráficos pelo menos de barras, linhas, tabela, combinados (tabela e linhas), "treemap, Scatter"," "Gauges", mapas geográficos);

Cláusula 26.º

Serviços de instalação

1. O adjudicatário deverá possuir, pelo menos, **1 (um) técnico certificado** em cada uma das **competências técnicas** nas principais áreas de integração da solução, a saber:
   - Técnico certificado em tecnologia CheckPoint;
   - Técnico certificado em tecnologia F5;
   - Técnico certificado em tecnologia HPE;
   - Técnico certificado em tecnologia Cisco;
   - Técnico certificado em tecnologia VMWare;
   - Técnico certificado em tecnologia Trend Micro;
   - Técnico certificado em tecnologia Microsoft;
   - Técnico certificado em tecnologia Veeam;
   - Técnico certificado - C|EH Certified Ethical Hacker (EC Council).
2. No âmbito dos serviços de instalação, configuração e integração na infraestrutura da entidade

adjudicante, deverão ser considerados:

2.1. Instalação das VMs em ambiente VMWare;

2.2. Instalação e configuração de todas as componentes necessárias ao cumprimento dos requisitos definidos nas especificações técnicas;

2.3. Configuração de todos os parâmetros necessários nos equipamentos existentes da infraestrutura da entidade adjudicante que permitam a correta monitorização dos eventos, incluindo a instalação dos agentes previstos para a monitorização dos servidores e aplicações;

2.4. Definição de intervalos e configuração de alarmística automatizada da disponibilidade de serviços e sistemas de segurança;

2.5. Definição e configuração de alarmística relativa a desvios comportamentais relativos à atividade percecionada nos eventos de segurança;

2.6. Definição e configuração de relatórios mensais (detalhados) e trimestrais (executivos) com informação relevante relativa aos eventos de segurança no contexto da entidade adjudicante.

Cláusula 27.º

Serviços de formação, consolidação e customização

1. Com vista à melhor rentabilização da solução, no âmbito da proposta apresentada, deverão ainda ser incluídos e prestados a título de formação, treino, consolidação e customização da integração e passagem de conhecimento, os serviços indicados nos pontos seguintes.
2. **Serviço de formação "on-job"** em horário laboral em full-time, por um **período mínimo de 1 (uma) semana**, ministrada em Língua Portuguesa;
3. **Serviços de consolidação e customização da integração da solução** com o objetivo de afinar, ajustar e otimizar as configurações e alertas para rentabilização máxima da solução e do ambiente em produção no IGeFE, I.P.
4. Os serviços indicados no ponto anterior devem incluir a monitorização e operação 24x7 durante um **período mínimo de 2 (dois) meses**, contados a partir de conclusão da implementação, com o seguinte enquadramento:

   4.1. Equipa 24x7 com 1 (uma) hora tempo de resposta com monitorização, suporte a gestão de alterações do serviço, considerando as seguintes atividades:

   - **Receção de alertas:** um alerta pode vir da plataforma SIEM ou via email;
   - **Análise de alertas:** uma vez recebido o alerta, os analistas avaliam o alerta e os dados associados fornecidos;
   - **Triagem de alertas**: com base em todas as informações recolhidas, os analistas seguem os *playbooks* padrão do SOC para detetar se o alerta é um incidente ou um falso positivo;
   - **Notificação de incidentes**: Caso seja um incidente, o IGeFE, I.P. é notificado para o seu ponto de contacto com todas as informações necessárias para que possa tomar as devidas ações;

- **Alertas críticos**: O SOC/NOC entrará em contato telefonicamente com os responsáveis do **IGeFE**;

4.2. Operação da infraestrutura de segurança em regime 8x5 que permita a correta customização da integração da solução proposta com a própria infraestrutura monitorizada, cobrindo as seguintes componentes:

- **Solução de segurança de perímetro** - Checkpoint (solução distribuída 2 datacenter (1 cluster + gateway + consola de gestão), considerando que no âmbito estão todas alterações necessárias à modernização da solução e/ou implementação de novos ambientes;
- **Solução de proteção aplicacional** - Balanceadores e WAF da F5 Networks (cluster com vários ambientes), considerando que no âmbito estão todas as alterações necessárias à modernização da solução e/ou implementação de novos ambientes;
- **Solução de comunicações de dados** - Switches de CORE (solução distribuída em dois datacenters com tecnologia Cisco e HPE), considerando que no âmbito estão todas as alterações necessárias à modernização da solução e/ou implementação de novos ambientes;
- **Solução de proteção de endpoints** - Tecnologia Trend Micro com APEX ONE com componentes de encriptação (instalada em todos os postos de trabalho e gerida por consola central), considerando que no âmbito estão todas as alterações necessárias à modernização da solução e/ou implementação de novos ambientes.

5. A entidade adjudicante disponibilizará o acesso remoto à infraestrutura durante o período de consolidação e customização da integração da solução, que terá a duração prevista no número 2 da cláusula 8.ª do presente caderno de encargos.

Cláusula 28.ª

Serviços de suporte e manutenção

O adjudicatário deve prestar os seguintes serviços de suporte e manutenção:

- Suporte do fabricante da solução implementada no regime de 24x7;
- Subscrição de fontes de informação (*feeds*) relativa a ameaças (*Threat Intelligence*) e indicadores de comprometimento (*IoC*) do fabricante da solução, contendo domínios maliciosos, reputação de IPs, hashes, etc..