



ASSOCIAÇÃO DE MUNICÍPIOS DO VALE DO SOUSA

(Castelo de Paiva, Felgueiras, Lousada, Paços de Ferreira, Paredes e Penafiel)

**CONCURSO PÚBLICO INTERNACIONAL PARA AQUISIÇÃO DE SERVIÇOS DE
IMPLEMENTAÇÃO DE SOLUÇÃO DE SEGURANÇA PARA ENDPOINT**

CADERNO DE ENCARGOS

- 2025 -

ÍNDICE

SECÇÃO I – CLÁUSULAS JURÍDICAS	3
CAPÍTULO I - DISPOSIÇÕES GERAIS.....	3
Cláusula 1. ^a - Objeto	3
Cláusula 2. ^a - Contrato.....	3
Cláusula 3. ^a - Prazos	4
Cláusula 4. ^a - Local de execução.....	4
Cláusula 5. ^a - Preço base e preço contratual.....	4
Cláusula 6. ^a - Condições de pagamento e faturação.....	4
CAPÍTULO II - OBRIGAÇÕES DAS PARTES	5
Cláusula 7. ^a - Obrigações gerais do Prestador de Serviços.....	5
Cláusula 8. ^a - Vínculo laboral dos trabalhadores afetos à execução do contrato	6
Cláusula 9. ^a - Dever de sigilo.....	6
Cláusula 10. ^a - Obrigações do Contraente Público.....	6
Cláusula 11. ^a - Tratamento e Proteção de Dados Pessoais.....	7
Cláusula 12. ^a - Liberação da caução.....	8
Cláusula 13. ^a - Gestor do contrato.....	8
CAPÍTULO III - VICISSITUDES CONTRATUAIS	9
Cláusula 14. ^a - Cessão da posição contratual do Prestador de Serviços.....	9
Cláusula 15. ^a - Sanções contratuais.....	9
Cláusula 16. ^a - Resolução do contrato pelo Contraente Público	9
Cláusula 17. ^a - Casos de Força Maior.....	10
Cláusula 18. ^a - Resolução do Contrato por parte do Prestador de Serviços	11
CAPÍTULO IV - DISPOSIÇÕES FINAIS	11
Cláusula 19. ^a - Deveres de Informação	11
Cláusula 20. ^a - Direitos de propriedade intelectual	11
Cláusula 21. ^a - Comunicações e notificações.....	11
Cláusula 22. ^a - Contagem dos prazos na fase de execução do contrato.....	12
Cláusula 23. ^a - Foro competente.....	12
Cláusula 24. ^a - Legislação aplicável	12
SECÇÃO II – CLÁUSULAS TÉCNICAS E FUNCIONAIS.....	13
Cláusula 25. ^a - Serviços a prestar.....	13
Cláusula 26. ^a - Conformidade dos serviços.....	17
Cláusula 27. ^a - Requisitos técnicos	17
Cláusula 28. ^a - Níveis de serviço	20
Cláusula 29. ^a - Forma de prestação dos serviços.....	21
Cláusula 30. ^a - Aceitação dos serviços prestados	22
Cláusula 31. ^a - Garantia técnica.....	22

CADERNO DE ENCARGOS

SECÇÃO I – CLÁUSULAS JURÍDICAS

CAPÍTULO I

DISPOSIÇÕES GERAIS

Cláusula 1.^a

Objeto

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual de **Aquisição de Serviços de Implementação de Solução de Segurança para Endpoint**, que tem por objeto principal a aquisição de serviços de implementação de uma solução de segurança para postos de trabalho e servidores (*Endpoint*), através de sistema de Security Operations Center (SOC), que inclui serviços de monitorização, análise e resposta a incidentes de segurança, antivírus de nova geração com recurso a inteligência artificial/*machine learning* e análise comportamental, e ainda o serviço gerido de deteção e reposta *threat hunting* 24/7, de acordo com as disposições constantes na secção II – Cláusulas Técnicas e Funcionais do presente Caderno de Encargos, promovido pela Associação de Municípios do Vale do Sousa (VALSOUSA), doravante designada por Contraente Público.

Cláusula 2.^a

Contrato

1. O contrato é composto pelo respetivo clausulado contratual e seus anexos, e integrará ainda os seguintes elementos:
 - 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 e anexos;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos sobre a proposta adjudicada prestados pelo Prestador de Serviços.
2. Sem prejuízo do disposto no número seguinte, em caso de divergência entre os vários documentos que integram o contrato, a prevalência é determinada pela ordem por que vêm enunciados no número anterior.
3. Os ajustamentos propostos pelo Contraente Público nos termos previstos no artigo 99.º do Código dos Contratos Públicos (doravante CCP), e aceites pelo Prestador de Serviços nos termos previstos no artigo 101.º do mesmo diploma legal, prevalecem sobre todos os documentos previstos no n.º 1 da presente cláusula.
4. Além dos documentos indicados no n.º 1, o Prestador de Serviços obriga-se também 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.
5. Persistindo dúvidas, aplicar-se-á o Código dos Contratos Públicos, na sua redação atual, e demais legislação portuguesa aplicável.

Cláusula 3.^a

Prazos

O contrato de prestação de serviços objeto do procedimento mantém-se em vigor pelo prazo de **36 (trinta e seis) meses**, a contar da outorga do contrato, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

Cláusula 4.^a

Local de execução

Os serviços são prestados nas instalações do Contraente Público, situadas em Lousada, ou noutro local que o mesmo venha a indicar para o efeito.

Cláusula 5.^a

Preço base e preço contratual

1. O preço máximo que o Contraente Público se dispõe a pagar pela presente aquisição de serviços, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, é de **480.000,00€ (quatrocentos e oitenta mil euros)**, acrescido do IVA à taxa legal em vigor.
2. O preço previsto no n.º 1 da presente cláusula inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao Contraente Público no presente Caderno de Encargos, incluindo despesas de alojamento, alimentação, deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.
3. O Contraente Público obriga-se a pagar ao Prestador de Serviços o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor.

Cláusula 6.^a

Condições de pagamento e faturação

1. As quantias devidas, nos termos da cláusula anterior, devem ser pagas no prazo de 60 (sessenta) dias, após a receção pelo Contraente Público da respetiva fatura, a qual só pode ser emitida, com periodicidade mensal, após o vencimento da obrigação respetiva.
2. A faturação a emitir pelo Prestador de Serviços assume a forma de faturas eletrónicas, com os requisitos legais, nomeadamente os resultantes do artigo 299º-B do CCP, sendo que a VALSOUSA utiliza uma solução de faturação eletrónica através de Intercâmbio Eletrónico de Dados (EDI), tendo selecionado a empresa Cegid YET - Your Electronic Transactions, Lda. para o fornecimento dessa mesma solução (acessível em <https://yetspace.com>, e com os seguintes contactos para apoio técnico aos fornecedores - e-mail: sales@yetspace.com - telefone: +351 253 149 253), de registo gratuito, devendo todas as faturas emitidas no âmbito do presente contrato ser enviadas por esta via.
3. Desde que devidamente emitida e observado o disposto no n.º 1, a fatura será paga através de transferência bancária (para o IBAN indicado pelo adjudicatário/fornecedor), devendo a mesma ser emitida em nome da Associação de Municípios do Vale do Sousa (VALSOUSA), com sede na Praça D. António Meireles, 45, 4620-130 Lousada, e cujo número de identificação fiscal (NIF) é o 502 599 189.
4. Cada fatura deverá, obrigatoriamente, identificar a designação do contrato, o número do respetivo compromisso financeiro, o prazo de pagamento (60 dias), a fase de execução a que diz respeito e quantia faturada.
5. Em caso de discordância por parte do Contraente Público quanto aos valores ou quantidades indicadas nas faturas, deve este comunicar ao Prestador de Serviços, por escrito, os respetivos fundamentos, ficando aquele obrigado a prestar os esclarecimentos necessários ou proceder à retificação da fatura.
6. O atraso em um ou mais pagamentos não determina o vencimento das restantes obrigações de pagamento.

7. Sem prejuízo da aplicação de outras penalidades ou sanções previstas no presente Caderno de Encargos ou determinadas por lei, o cumprimento defeituoso da prestação dos serviços terá um efeito suspensivo sobre a faturação e sobre o pagamento até à total regularização da situação.

CAPÍTULO II

OBRIGAÇÕES DAS PARTES

Cláusula 7.^a

Obrigações gerais do Prestador de Serviços

1. Nos termos do contrato a celebrar, o Prestador de Serviços obriga-se, durante o período da sua execução, à realização de todas as operações necessárias ao integral cumprimento do objeto do contrato.

2. Sem prejuízo de outras obrigações previstas na legislação aplicável ou nas cláusulas contratuais, da celebração do contrato decorrem para o Prestador de Serviços as seguintes obrigações principais:

- a) Prestar os serviços em perfeitas condições e para os fins a que se destinam, dentro dos prazos definidos no presente Caderno de Encargos e conforme as condições aí estipuladas, bem como nos demais documentos contratuais;
- b) Assegurar o cumprimento dos requisitos técnicos, funcionais, ambientais e níveis de serviço, tal como previstos no presente Caderno de Encargos e na legislação aplicável;
- c) Garantir os serviços prestados, de acordo com as condições definidas no presente Caderno de Encargos e demais documentos contratuais e disposições legais em vigor;
- d) Recorrer a todos os meios humanos, materiais, técnicos e criativos que sejam necessários à execução do contrato;
- e) Comunicar ao Contraente Público, logo que tenha conhecimento, os factos que tornem total ou parcialmente impossível a prestação dos serviços objeto do contrato, ou o cumprimento de qualquer outra das suas obrigações, nos termos do contrato celebrado;
- f) Não alterar as condições da prestação dos serviços fora dos casos previstos no presente Caderno de Encargos;
- g) Prestar de forma correta e fidedigna as informações referentes às condições em que são prestados os serviços, bem como conceder todos os esclarecimentos solicitados pelo Contraente Público;
- h) Comunicar qualquer facto que ocorra durante a execução do Contrato relacionado com a sua denominação social, os seus representantes legais, a sua situação jurídica, a sua situação comercial e outras, com relevância para a prestação dos serviços;
- i) Possuir todas as autorizações, consentimentos, aprovações, patentes, registos e licenças necessários ao pontual cumprimento das obrigações assumidas;
- j) Cooperar com o Contraente Público, mediante solicitação, designadamente nas seguintes situações:
 - i. Quando um titular de dados pessoais exerça os seus direitos ou cumpra as suas obrigações nos termos da legislação aplicável, relativamente aos dados pessoais tratados pelo Prestador de Serviços em representação do Contraente Público;
 - ii. Quando o Contraente Público deva cumprir ou dar sequência a qualquer avaliação, inquérito, notificação ou investigação da Comissão Nacional de Proteção de Dados ou entidade administrativa com atribuições e competências legais equiparáveis.

3. O Prestador de Serviços fica sujeito, com as devidas adaptações, às exigências legais, obrigações do fornecedor e prazos aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código dos Contratos Públicos, na sua redação atual, bem como toda a legislação e regulamentação portuguesa e europeia aplicável.

Cláusula 8.^a

Vínculo laboral dos trabalhadores afetos à execução do contrato

1. Nos termos do disposto no n.º 1 do artigo 419.º-A, aplicável por força do n.º 2 do artigo 451.º, ambos do CCP, o Prestador de Serviços obriga-se a colocar a executar o contrato trabalhadores em regime de contrato de trabalho sem termo.
2. O disposto no n.º 1 não se aplica aos trabalhadores com contrato a termo de substituição celebrado nas situações previstas nas alíneas a) a d) do n.º 2 do artigo 140.º do Código do Trabalho.
3. O disposto no n.º 1 não se aplica a trabalhadores que executem tarefas ocasionais ou serviços específicos e não duradouros no âmbito da execução da prestação.

Cláusula 9.^a

Dever de sigilo

1. O Prestador de Serviços obriga-se a não divulgar quaisquer informações e documentação, técnica e não técnica, comercial ou outra, relativa ao Contraente Público, de que venha a ter conhecimento ao abrigo ou em relação com a execução do contrato, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos.
2. O Prestador de Serviços obriga-se também a não utilizar as informações obtidas para fins alheios à execução do contrato.
3. 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.
4. Exclui-se do dever de sigilo previsto a informação e a documentação que seja comprovadamente do domínio público à data da respetiva obtenção pelo Prestador de Serviços 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.
5. O Prestador de Serviços obriga-se a remover e destruir no termo final do prazo contratual todo e qualquer registo, em papel ou eletrónico, que contenha dados ou informações referentes ou obtidas na execução do contrato e que o Contraente Público lhe indique para esse efeito.
6. O dever de sigilo mantém-se em vigor indefinidamente, até autorização expressa do contraente público, 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.
7. O Prestador de Serviços não pode utilizar o logótipo, ou qualquer outro sinal distintivo do Contraente Público, sem o consentimento prévio deste.

Cláusula 10.^a

Obrigações do Contraente Público

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, o Contraente Público obriga-se a fiscalizar a execução do objeto do contrato de forma profissional e competente, utilizando os conhecimentos técnicos, a diligência e o zelo.
2. Constituem, ainda, obrigações do Contraente Público:
 - a) Nomear um responsável pela gestão do contrato para efeitos de comunicações com o Prestador de Serviços, e comunicar quaisquer alterações dessa nomeação;
 - b) Monitorizar e supervisionar a aplicação das condições e termos contratuais;
 - c) Monitorizar a qualidade dos serviços prestados;
 - d) Comunicar, em tempo útil, os aspetos relevantes que tenham impacto no cumprimento do contrato;

- e) Disponibilizar o acesso às instalações para a entrega dos produtos fornecidos;
- f) Efetuar o pagamento contratualmente devido dentro dos prazos fixados.

Cláusula 11.ª

Tratamento e Proteção de Dados Pessoais

1. O Prestador de Serviços compromete-se a assegurar o cumprimento das obrigações decorrentes do Regulamento Geral de Proteção de Dados (doravante designado RGPD), aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, e da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, daquele regulamento, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e demais legislação que lhe seja aplicável relativa a dados pessoais, durante a execução do contrato, assim como após o termo da vigência do período de execução contratual, designadamente:

- a) Utilizar os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pelo Contraente Público, única e exclusivamente para as finalidades previstas no contrato;
- b) Manter os dados pessoais estritamente confidenciais, cumprindo e garantindo o cumprimento do dever de sigilo profissional relativamente aos mesmos;
- c) Cumprir quaisquer regras relacionadas com o tratamento de dados pessoais a que o Contraente Público esteja especialmente vinculado;
- d) Pôr em prática as medidas técnicas e organizativas necessárias à proteção dos dados pessoais tratados por conta do Contraente Público, nomeadamente 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;
- e) Prestar ao Contraente Público toda a colaboração de que este careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais, efetuado ao abrigo do contrato;
- f) Manter o Contraente Público informado em relação ao tratamento de dados pessoais, obrigando-se a comunicar de imediato qualquer situação que possa afetar o tratamento dos mesmos, ou que, de algum modo, possa dar origem ao incumprimento das disposições legais em matéria de proteção de dados pessoais;
- g) Assegurar o cumprimento do RGPD e demais legislação relativa à proteção de dados, por todos os seus colaboradores, incluindo toda e qualquer pessoa singular ou coletiva que preste serviços ao Prestador de Serviços, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido entre o Prestador de Serviços e o referido colaborador;
- h) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
- i) Não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou, por qualquer outra forma, colocar à disposição de terceiros os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pelo Contraente Público ao abrigo do contrato, exceto quando tal lhe tenha sido expressamente comunicado, por escrito, por este ou quando decorra do cumprimento de uma obrigação legal;
- j) Adotar as medidas de segurança previstas no artigo 32.º do RGPD, que assegurem a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços de tratamento de dados pessoais e implementar um processo para testar, apreciar e avaliar regularmente a eficácia destas medidas;
- k) Prestar a assistência necessária ao Contraente Público no sentido de permitir que este cumpra a obrigação de dar resposta aos pedidos dos titulares dos dados, tendo em vista o exercício dos direitos previstos no RGPD, nomeadamente o direito de acesso, retificação, oposição, apagamento, limitação e portabilidade dos seus dados pessoais;

- I) Garantir a eficácia de mecanismo de notificação efetivo em caso de violação de dados pessoais para efeitos do cumprimento do previsto no artigo 33.º do RGPD.
2. O Prestador de Serviços será responsável por qualquer prejuízo em que o Contraente Público venha a incorrer em consequência do tratamento de dados pessoais, por parte do mesmo e/ou dos seus trabalhadores, colaboradores, prestadores de serviços ou fornecedores, em violação das normas legais aplicáveis.
3. Os dados pessoais a tratar no âmbito do contrato são os previstos no n.º 1 do artigo 4.º do RGPD.
4. O tratamento de dados pessoais a realizar pelo Prestador de Serviços é efetuado de acordo com as instruções do responsável pelo tratamento de dados, ou seja, o Contraente Público.
5. O Prestador de Serviços deve declarar, sob compromisso de honra, de que possui as condições necessárias e suficientes à execução das medidas técnicas e organizativas previstas no RGPD.

Cláusula 12.ª

Liberação da caução

1. No caso em que não haja obrigações de correção de defeitos pelo Prestador de Serviços, designadamente obrigações de garantia, o Contraente Público deve promover a liberação integral da caução destinada a garantir o exato e pontual cumprimento das obrigações contratuais no prazo de 30 dias após o cumprimento de todas as obrigações do Prestador de Serviços.
2. No caso em que haja obrigações de correção de defeitos pelo Prestador de Serviços, designadamente obrigações de garantia, sujeitas a um prazo igual ou inferior a três anos, o Contraente Público deve promover a liberação integral da caução destinada a garantir o exato e pontual cumprimento das obrigações contratuais no prazo de 30 dias após o termo do respetivo prazo, situação aplicável apenas nos serviços que incorporem períodos de garantia, por exemplo, serviços de reparação ou serviços digitais.
3. A liberação da caução depende da inexistência de defeitos da prestação do Prestador de Serviços ou da correção daqueles que hajam sido detetados até ao momento da liberação, situação aplicável apenas nos serviços que incorporem períodos de garantia, por exemplo, serviços de reparação ou serviços digitais, sem prejuízo de o Contraente Público poder decidir diferentemente, designadamente por considerar que os defeitos identificados e não corrigidos são de pequena importância e não justificam a não liberação.
4. Decorrido o prazo previsto nos números anteriores para a liberação da caução sem que esta tenha ocorrido, o Prestador de Serviços pode notificar o Contraente Público para que este cumpra a obrigação de liberação da caução, ficando autorizado a promovê-la, a título parcial ou integral, se, 15 dias após a notificação o Contraente Público não tiver dado cumprimento à referida obrigação.
5. A mora na liberação, total ou parcial, da caução confere ao Prestador de Serviços o direito de indemnização, designadamente pelos custos adicionais por este incorridos com a manutenção da caução prestada por período superior ao que seria devido.

Cláusula 13.ª

Gestor do contrato

1. Para cumprimento do artigo 290.º-A do CCP, o Contraente Público designará um gestor do contrato, com a função de acompanhar permanentemente a execução deste, podendo ser lhe delegados poderes para a adoção das medidas corretivas que se revelem adequadas, no caso de detetar desvios, defeitos, ou outras anomalias na execução do contrato, exceto em matéria de modificação e cessação do contrato.
2. A indicação do gestor do contrato, em nome o Contraente Público, constará do clausulado do contrato, nos termos do disposto na alínea i) do n.º 1 do artigo 96.º do CCP.

CAPÍTULO III

VICISSITUDES CONTRATUAIS

Cláusula 14.ª

Cessão da posição contratual do Prestador de Serviços

1. Além da situação prevista na alínea a) do n.º 1 do artigo 318.º do CCP, o Prestador de Serviços pode ceder a sua posição contratual, na fase de execução do contrato, mediante autorização do Contraente Público.
2. Para efeitos da autorização a que se refere o número anterior, o Prestador de Serviços deve apresentar uma proposta fundamentada e instruída com os documentos previstos no n.º 2 do artigo 318.º do CCP.
3. O Contraente Público deve pronunciar-se sobre a proposta do Prestador de Serviços no prazo de 30 (trinta) dias a contar da respetiva apresentação, desde que regularmente instruída, considerando-se o referido pedido rejeitado se, no termo desse prazo, o mesmo não se pronunciar expressamente.
4. Em caso de incumprimento pelo Prestador de Serviços que reúna os pressupostos para a resolução do contrato, este cederá a sua posição contratual ao concorrente do procedimento pré-contratual que antecedeu a celebração do contrato que venha a ser indicado pelo Contraente Público, de acordo com o estabelecido no artigo 318.º-A do CCP.
5. A cessão da posição contratual a que se refere o número anterior opera por mero efeito do ato do Contraente Público, sendo eficaz a partir da data por este indicada.

Cláusula 15.ª

Sanções contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, o Contraente Público pode exigir do fornecedor o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, nos termos da legislação em vigor.
2. O valor acumulado das sanções contratuais a aplicar não poderá exceder o limite máximo de 20% do preço contratual. Nos casos em que seja atingido o limite de 20% e o Contraente Público decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.
3. Em caso de resolução do contrato, por incumprimento do Prestador de Serviços, o Contraente Público pode exigir-lhe uma sanção contratual de até aos limites indicados no número anterior.
4. Ao valor da sanção contratual previsto no número anterior são deduzidas as importâncias pagas pelo Prestador de Serviços ao abrigo do n.º 1, relativamente aos serviços objeto do contrato cujo atraso na respetiva conclusão tenha determinado a respetiva resolução.
5. O Contraente Público pode compensar os pagamentos devidos ao abrigo do contrato com as sanções contratuais devidas nos termos da presente cláusula.
6. As penas pecuniárias previstas na presente cláusula não obstam a que o Contraente Público exija uma indemnização nos termos gerais, nomeadamente pelos prejuízos decorrentes da adoção de novo procedimento de formação do contrato ou danos excedentes.

Cláusula 16.ª

Resolução do contrato pelo Contraente Público

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o Contraente Público pode resolver o contrato, a título sancionatório, no caso de o Prestador de Serviços violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente no caso de atraso, total ou parcial, superior a 30 (trinta) dias na prestação dos serviços objeto do contrato ou o Prestador de Serviços declarar por escrito que o atraso na prestação excederá esse prazo.

2. O contrato pode também ser resolvido pelo Contraente Público caso se verifique alguma das seguintes situações, as quais são desde já entendidas como situações de incumprimento grave e culposo por parte do Prestador de Serviços:

- a) Quando se verificar reiterada inobservância das disposições do contrato ou má-fé do Prestador de Serviços;
- b) Prestação de falsas declarações;
- c) Estado de falência ou insolvência;
- d) Cessaç o da atividade;
- e) Condenaç o, por senten a transitada em julgado, por infra  o que afete a idoneidade profissional do Prestador de Servi os e desde que n o tenha ocorrido reabilita  o judicial.

3. O direito de resolu  o referido no n mero anterior exerce-se mediante declara  o escrita enviada ao Prestador de Servi os e n o implica a repeti  o das presta  es j  realizadas pelo mesmo nos termos previstos no presente Caderno de Encargos, a menos que tal seja expressamente determinado pelo Contraente P blico.

Cl usula 17. 

Casos de For a Maior

1. N o podem ser impostas san  es contratuais ao Prestador de Servi os, nem   havida como incumprimento, a n o realiza  o pontual das presta  es contratuais a cargo de qualquer das partes que resulte de caso de for a maior.

2. Para efeitos do contrato, s  s o consideradas de for a maior as circunst ncias que, cumulativamente e em rela  o   parte que as invoca:

- a) Impossibilitem o cumprimento das obriga  es emergentes do contrato;
- b) Sejam alheias   sua vontade;
- c) N o fossem por ela conhecidas ou previs veis   data da celebra  o do contrato;
- d) N o lhe seja razoavelmente exig vel contornar ou evitar os efeitos produzidos por aquelas circunst ncias.

3. N o constituem for a maior, designadamente, quando aplic veis:

- a) Circunst ncias que n o constituam for a maior para os subcontratados do Prestador de Servi os, na parte em que intervenham;
- b) Greves ou conflitos laborais limitados  s sociedades do Prestador de Servi os ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
- c) Determina  es governamentais, administrativas ou judiciais de natureza sancionat ria, ou de outra forma resultantes do incumprimento pelo Prestador de Servi os de deveres ou  nus que sobre ele recaiam;
- d) Manifesta  es populares devidas ao incumprimento pelo Prestador de Servi os de normas legais;
- e) Inc ndios ou inunda  es com origem nas instala  es do Prestador de Servi os cuja causa, propaga  o ou propor  es se devam a culpa ou neglig ncia sua ou ao incumprimento de normas de seguran a;
- f) Avarias nos sistemas inform ticos ou mec nicos do Prestador de Servi os n o devidas a sabotagem;
- g) Eventos que estejam ou devam estar cobertos por seguros.

4. A parte que invocar caso de for a maior deve comunicar e justificar tal situa  o   outra parte, logo ap s a sua ocorr ncia, bem como informar o prazo previs vel para restabelecer o cumprimento das obriga  es contratuais.

5. A suspensão, total ou parcial, do cumprimento pelo Prestador de Serviços das suas obrigações contratuais fundada em força maior, por prazo superior a 30 (trinta) dias, autoriza o Contraente Público a resolver o contrato ao abrigo do n.º 1 do artigo 335.º do CCP, não tendo o Prestador de Serviços direito a qualquer indemnização.

Cláusula 18.ª

Resolução do Contrato por parte do Prestador de Serviços

1. O Prestador de Serviços pode resolver o contrato com os fundamentos previstos no artigo 332.º do CCP.
2. O direito de resolução é exercido por via judicial, nos termos da Cláusula 23.ª.
3. A resolução do contrato não determina a repetição das prestações já realizadas pelo Prestador de Serviços, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do CCP.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Cláusula 19.ª

Deveres de Informação

Cada uma das partes deve informar, sem demora a outra, de quaisquer circunstâncias que cheguem ao seu conhecimento e possam afetar os respetivos interesses na execução do contrato que, previsivelmente, impeçam o cumprimento ou o cumprimento tempestivo de qualquer uma das suas obrigações, de acordo com a boa-fé.

Cláusula 20.ª

Direitos de propriedade intelectual

1. Correm integralmente por conta do Prestador de Serviços os encargos ou a responsabilidade civil decorrentes da incorporação em qualquer dos serviços objeto do contrato, ou da utilização nesses mesmos serviços, de materiais, de *hardware*, de *software* ou de outros que respeitem a quaisquer patentes, licenças, marcas, desenhos registados e outros direitos de propriedade industrial ou direitos de autor ou conexos.
2. Se o Contraente Público vier a ser demandado por ter infringido, na execução do contrato ou na posterior utilização dos serviços objeto do mesmo, qualquer dos direitos referidos no número anterior, terá direito de regresso contra o Prestador de Serviços por quaisquer quantias pagas, seja a que título for.
3. São da responsabilidade do Prestador de Serviços quaisquer encargos decorrentes da utilização, na execução do contrato, de marcas registadas, patentes registadas ou licenças.
4. Os encargos e a responsabilidade civil perante terceiros decorrentes dos factos mencionados nos n.ºs 1 e 2 não correm por conta do Prestador de Serviços, se este demonstrar que os mesmos são imputáveis ao Contraente Público ou a terceiros que não sejam seus subcontratados.

Cláusula 21.ª

Comunicações e notificações

1. Quaisquer comunicações ou notificações entre o Contraente Público e o Prestador de Serviços relativos ao contrato, seguem o regime previsto no artigo 469.º do CCP, sem prejuízo do disposto no número seguinte.

2. As comunicações e as notificações dirigidas ao Contraente Público, efetuadas através de correio eletrónico ou outro meio de transmissão escrita e eletrónica de dados, têm de ser efetuadas até às 17h00 do dia a que digam respeito, sob pena de se considerarem efetuadas às 10h00 do dia útil imediatamente seguinte.

Cláusula 22.ª

Contagem dos prazos na fase de execução do contrato

À contagem de prazos na fase de execução do contrato, e salvo disposição expressa em contrário, são aplicáveis as seguintes regras:

- a) Não se inclui na contagem do prazo o dia em que ocorrer o evento a partir do qual o mesmo começa a correr;
- b) Os prazos são contínuos, não se suspendendo nos sábados, domingos e feriados;
- c) O prazo fixado em semanas, meses ou anos, a contar de certa data, termina às 24 horas do dia que corresponda, dentro da última semana, mês ou ano, a essa data, mas se no último mês não existir dia correspondente o prazo finda no último dia desse mês;
- d) O prazo que termine em sábado, domingo, feriado ou em dia em que o serviço perante o qual deva ser praticado o ato que não esteja aberto ao público, ou não funcione durante o período normal, transfere-se para o 1.º dia útil seguinte.

Cláusula 23.ª

Foro competente

Para todas as questões emergentes do presente contrato, será competente o Juízo de contratos públicos do Tribunal Administrativo e Fiscal do Porto, de acordo com o n.º 2 do artigo 8.º do Decreto-Lei n.º 174/2019, de 13 de dezembro.

Cláusula 24.ª

Legislação aplicável

- 1. O contrato é regulado pela legislação portuguesa.
- 2. Sem prejuízo de outras leis e regulamentos especialmente aplicáveis, a tudo o que não esteja expressamente previsto ou regulado no presente Caderno de Encargos, e nas demais regulamentações do procedimento pré-contratual e do contrato, aplica-se o regime previsto no CCP, na sua atual redação, e demais legislação aplicável.

SECÇÃO II – CLÁUSULAS TÉCNICAS E FUNCIONAIS

Cláusula 25.^a

Serviços a prestar

1. Pretende-se a aquisição de serviços de Detecção e Resposta a Incidentes de Segurança em todos os ativos, dinamicamente ajustada em função da evolução das ameaças e em articulação com as entidades promotoras de Cibersegurança, como a da Rede Nacional CSIRT (*Computer Security Incident Response Team*) e do Centro Nacional de Cibersegurança (CNCS), em cumprimento com os requisitos legais do Decreto-Lei n.º 65/2021, de 30 de julho, e instruções conexas do CNCS, e demais legislação nacional e europeia aplicável.
2. O Prestador de Serviços obriga-se a entregar ao Contraente Público os serviços objeto do contrato com as características, especificações e requisitos técnicos previstos nesta secção.
3. Na materialização da sua estratégia de cibersegurança e em resposta ao contexto atual de ameaças digitais, pretende-se adquirir uma solução de *Extended Detection and Response* (XDR) que deverá incluir as capacidades e funcionalidades descritas abaixo:
 - a) Instalação de, pelo menos, 1350 (mil trezentos e cinquenta) postos de trabalho/servidores (*endpoints*);
 - b) Prevenção contra *exploits*, incluindo aqueles que utilizam vulnerabilidades do tipo Zero-Day;
 - c) Prevenção contra a execução de *malware*, sem requerer qualquer conhecimento prévio;
 - d) Capacidade de restringir a execução de determinados processos;
 - e) Capacidade de proteger contra *ransomware*;
 - f) Controlar dispositivos USB;
 - g) *Disk Encryption*;
 - h) *Host Firewall*;
 - i) *Malware Scanning*;
 - j) Módulo de *Endpoint Detection and Response* (EDR);
 - k) Módulo de *User Entity Behavior Analytics* (UEBA).
4. Os requisitos da solução e serviço são detalhados nos números seguintes, em cada uma das suas componentes, sendo que todas as licenças de software/subscrições e serviços fornecidas deverão ter uma duração de 36 meses.
5. Na componente **Gestão**, a solução proposta deve:
 - a) Ser gerida através de uma interface gráfica *web*;
 - b) Ter uma gestão centralizada baseada em *cloud*;
 - c) 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*;
 - d) Manter um *audit log* das seguintes ações dos administradores: isolar máquina, terminar processo, *upgrade* de agente, *uninstall* do agente, adicionar/remover artefacto de *whitelist* e *blacklist*;
 - e) Suportar a atualização de *software* dos agentes de *endpoint* diretamente a partir da *cloud*;
 - f) Poder exportar os seus *logs* em formato *syslog* para qualquer solução de gestão de *logs*.
6. Na componente **Prevenção de Exploits**, a solução proposta deve:

- a) 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;
- b) 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.;
- c) 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;
- d) Prevenir ou bloquear uma técnica de *exploit*, 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;
- e) Utilizar módulos de técnicas de *exploit* para prevenir ou bloquear *exploits*, não devendo basear a prevenção ou bloqueio de *exploits* em assinaturas, reputação e heurísticas dos ficheiros;
- f) 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*, e deve ter impacto mínimo no desempenho através da utilização de um agente leve e não intrusivo que pode ser totalmente invisível para o utilizador;
- g) Proteger de forma simultânea todas as aplicações e processos do *endpoint* contra técnicas de *exploit*;
- h) 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;
- i) Conseguir proteger contra *exploits* para MacOS e Linux, como por exemplo “*local privilege escalation*”;
- j) Deve ser possível criar exceções de forma manual para técnicas de *exploit* específicas em processos específicos, e esta funcionalidade deve estar disponível em Windows, Linux e Mac.

7. Na componente **Prevenção de Malware**, a solução proposta deve:

- a) Suportar proteção contra a execução de executáveis maliciosos;
- b) Garantir a funcionalidade de monitorização ou aprendizagem do ambiente onde está instalado (i.e., processos e aplicações instaladas e a correr nos *endpoints*), e esta deverá ser utilizada na fase inicial de instalação e configuração;
- c) Ter a capacidade de controlar o que pode ser executado no *endpoint*, a partir de onde pode ser executado e com que parâmetros;
- d) Prevenir um processo de lançar qualquer processo legítimo que possa ser utilizado para fins maliciosos, e esta técnica é muitas vezes utilizada em *ransomware* e outros *malwares* para fazer *bypass* à segurança do *endpoint*;
- e) 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);
- f) Ser capaz de prevenir a execução de *malware* através da análise de comportamentos desencadeados pelo *malware*;
- g) Garantir a possibilidade de configurar *whitelists* globais para permitir a execução de certos ficheiros executáveis;
- h) Ser capaz de criar regras de exclusão das capacidades de proteção para *endpoints* específicos;

- i) Detetar e bloquear *malware* através do uso de *machine learning* e não deve utilizar assinaturas locais independentemente do sistema operativo;
- j) Ser capaz de analisar ficheiros do tipo mach-o, ELF e APK;
- k) Monitorizar os diferentes processos bem como as suas relações e origens (*Parent processes*) de forma a ser capaz de bloquear processos com comportamento malicioso;
- l) Permitir agendar *malware scans* para Windows, Linux e Mac;
- m) Proteger contra tentativas de adulteração, incluindo modificação e/ou *disable* do agente.

8. Na componente **Requisitos Adicionais**, a solução proposta deve:

- a) 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*;
- b) Conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do *malware*;
- c) Garantir a capacidade de efetuar análises estáticas (*machine learning*) em modo offline para Windows, Linux e macOS;
- d) 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;
- e) Conseguir que o módulo de análise de comportamentos de *ransomware* opere em modo de notificação ou de prevenção;
- f) Poder bloquear qualquer dispositivo USB externo que se conecte a um *endpoint* monitorizado pela solução, assim como bloquear determinado tipo de dispositivo USB, mas permitir apenas dispositivos de um vendedor específico ou com um *Serial Number* específico, e ser possível criar políticas apenas temporárias;
- g) 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;
- h) Disponibilizar na visão de cada incidente, informação sobre a classificação de cada *hash*;
- i) Suportar e proteger os seguintes sistemas operativos:
 - i. Android 8, 9, 10, 11, 12, 13, 14 e 15;
 - ii. iOS e iPadOS 15, 16;
 - iii. Debian 9, 10, 11 e 12;
 - iv. CentOS 6, 7, 8 e 9;
 - v. Oracle 6, 7, 8 e 9;
 - vi. Red Hat 6, 7, 8 e 9;
 - vii. SUSE 12 e 15;
 - viii. Ubuntu 12, 14, 16, 18, 20, 22 e 24;
 - ix. macOS 10.15, 11.x, 12.x, 13 ventura, 14 sonoma e 15 sequoia;
 - x. Windows 7, 8, 10 e 11;
 - xi. Windows Server 2008R2, 2012, 2016, 2019, 2022 e 2025.
- j) Ser capaz, no caso de não existir ligação à internet, de manter a cache dos dados coletados pelo modulo de EDR localmente, mesmo que seja feito um *reboot*;
- k) Ter capacidade de monitorizar, continuamente, toda a atividade dos *endpoints*, nomeadamente informação relativa a ações sobre: processos, ficheiros, tráfego de rede, *registry*, RPC Calls, System Calls, *event logs* de segurança e memória. A solução não deve estar dependente de eventos específicos para recolher continuamente todos os dados

mencionados. É obrigatório reter toda a informação independentemente da existência de incidentes de segurança;

- l) Ser capaz, com base na informação disponível, 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;
- m) 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;
- n) Ser capaz, quando diferentes alertas estão relacionados, de os agregar automaticamente num único incidente;
- o) Agregar diferentes incidentes num único de forma manual;
- p) Alterar a severidade de um incidente (ex: passar de *Medium* para *High*);
- q) Ser capaz, quando é identificado um novo incidente, 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;
- r) Indicar, para cada incidente, 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 notas para os analistas poderem colaborar entre si;
- s) Mapear os diferentes alertas para a Framework Mitre ATT&CK;
- t) Aprender o comportamento de cada máquina e criar perfis por *endpoint* de forma a ser capaz de identificar comportamentos anómalos;
- u) Aprender o comportamento de cada utilizador e criar perfis por utilizador de forma a ser capaz de identificar comportamentos anómalos;
- v) Identificar o perfil comportamental de todas as máquinas com e sem agente instalado;
- w) Ser capaz, com base na aprendizagem comportamental para cada máquina e utilizador, de gerar automaticamente alarmística para estes cenários:
 - i. sessão rara de SSH;
 - ii. uso de comandos fora do comum (arp -a, ipconfig, etc);
 - iii. *scripts* raros a comunicar com *hosts* externos;
 - iv. enumeração de contas de domínio;
 - v. pesquisa por ficheiros locais com passwords;
 - vi. login anormal via RDP;
 - vii. comando de *powershell* suspeito.
- x) Ter capacidade de reverter automaticamente alterações feitas na máquina por determinado *malware*, assim como listar as alterações feitas por qualquer processo malicioso e permitir reverter essas alterações;
- y) Disponibilizar uma funcionalidade de identificação de ameaças avançada que permita a melhor cobertura para vetores de ameaças de identidade furtivos, incluindo contas comprometidas e ameaças internas.

9. Na componente **Funcionalidades do agente para contenção de incidentes**, a solução proposta deve:

- a) Ter a possibilidade de efetuar *blacklists* e *whitelists* a *hashes*;
- b) Ter a possibilidade fazer quarentena a determinados processos;

- c) Permitir, durante a investigação de um incidente, isolar da rede máquinas infetadas;
- d) 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;
- e) Ter uma funcionalidade de Live Terminal, onde o analista possa aceder remotamente às máquinas de forma a: gerir os processos e ficheiros, correr *scripts* e aceder à linha de comandos da máquina;
- f) Permitir automatizar o processo de resposta a incidentes;
- g) Ter a possibilidade de criação de regras, para definir as ações que a plataforma deve tomar autonomamente para determinado tipo de incidente. Exemplos: correr um *script*, terminar uma ligação e isolar uma máquina;
- h) Ter capacidade de criar regras de correlação personalizadas que permitem detetar ataques retroativamente;
- i) Incluir uma linguagem de consulta avançada que suporte *wildcards*, expressões regulares, agregação de dados, manipulação de campos e valores, agregação de dados de fontes diferentes e visualização de dados.

Cláusula 26.ª

Conformidade dos serviços

Os serviços objeto do contrato devem ser prestados em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua prestação.

Cláusula 27.ª

Requisitos técnicos

O Prestador de Serviços deve assegurar os requisitos técnicos explicitados nos termos seguintes:

1. Dispor de um Centro de Resposta a Incidentes de Cibersegurança que incorpore uma equipa a operar 24 horas x 7 dias x 365 dias por ano, com capacidade para:
 - a) Resposta rápida a incidentes de segurança;
 - b) Análise contínua de *assets* expostos;
 - c) Elaboração de *playbooks* e *uses cases*;
 - d) Monitorização de ameaças com rápida resposta;
 - e) Análise de *emails* suspeitos;
 - f) Gestão de SIEM/SOAR.
2. Este centro deve possuir redundância geográfica em território nacional, com distância superior a 200 kms entre locais, para assegurar a continuidade de negócio.
3. Deve dispor, ainda, de 2 salas de crise em território nacional, contíguas ao centro referido no n.º 1, com distância superior a 200 km entre si.
4. Dispor de uma equipa, normalmente designada por PurpleTeam, que assegure a definição, realização e concretização de testes de penetração, garantindo a exploração de vulnerabilidades de ponto de vista de um atacante, desencadeando contramedidas, identificando as mitigações para resolução de pontos de falha identificados.
5. Dispor de valências de Gestão de Ameaças através de abordagem proativa que permita:
 - a) Identificação de vulnerabilidades;
 - b) Classificação do risco;
 - c) Engenharia reversa de *malware*;

- d) Produção de IOC (*Indicator of Compromise*) e interligação com outras *feeds*;
 - e) Investigação Forense, execução de DFIR (*Digital Forensics and Incident Response*);
 - f) Monitoração de *Deep & Dark Web*;
 - g) Monitoração e proteção da Marca e domínios do Contraente Público;
 - h) Busca por credenciais expostas.
6. Gestão de Incidentes de Segurança, garantindo que:
- a) Os mesmos são gerados e analisados de acordo com a taxonomia ENISA;
 - b) A sua resolução seja pela via de ações automatizadas de execução imediata, com base em regras e *use case* definidos como base do *framework* MITRE ATT&CK.
7. Análise de vulnerabilidades até 190 (cento e noventa) *assets* (ex: servidores), com as seguintes componentes:
- 1. Pré-análise de potenciais vulnerabilidades dos servidores na rede, incluindo *Cloud* e Infraestruturas de Virtualização;
 - 2. Efetuar priorização face a risco;
 - 3. Dispor de integração com *Feeds* de Ameaças e de novas metodologias de ataques identificadas mundialmente;
 - 4. Dispor de mecanismos de automação e atualizações identificadas pelos diferentes fornecedores;
 - 5. Recorrer a *Light Agents* suportados em ambientes Windows, Linux e macos;
 - 6. Recorrer a *Dashboards* em tempo real;
 - 7. Recorrer a ferramentas sistematizadas de execução de projetos de remediação, garantindo a coordenação de diferentes ações e equipas.
8. Dispor de serviço de *Deception* que permita criar armadilhas como *honeypots*, utilizadores *honey*, credenciais *honey* e arquivos *honey*, sendo que todos são criados para identificar comportamento malicioso no início da cadeia de ataque.
9. Dispor de processo de gestão de crise sempre a escalar a fim de conter ou mitigar efeitos de ataques, envolvendo as valências necessárias para tal.
10. Utilizar uma abordagem unificada que permita criar regras e *use cases* automáticos, orquestrando agentes e fontes de *log* por forma a responder de um modo automático a vários cenários de potenciais ataques, e para tal:
- a) O serviço deve ser suportado numa plataforma agregada de SIEM + SOAR de nova geração com inteligência artificial, integrada numa única plataforma de Gestão, garantindo o apresentado no número seguinte;
 - b) Implementação do serviço com base numa análise “MaGMa” (*Management, Growth and Metrics & assessment*) e respetiva realização do mapeamento MITRE da infraestrutura protegida do Contraente Público.
11. Dispor de uma plataforma SIEM multifuncional, com as seguintes características:
- a) Capacidade de monitorização até 1350 (mil trezentos e cinquenta) ativos;
 - b) Ser baseado numa plataforma em *cloud* com elevada escalabilidade;
 - c) Dispor de um agente para instalar nos sistemas Windows, Linux e MacOS, integrável no SIEM para análise de servidores, estações de trabalho, portáteis e dispositivos móveis.
 - d) *Embedded Threat Intelligence* – dispor de bibliotecas de ameaças, complementada com valências de *machine learning* e automação para permitir a redução de esforço e aceleração das atividades de análise e tratamento;

- e) NTA - *Network Traffic Analysis* – permitir visibilidade da rede com cobertura de deteção completa para reconhecer e avaliar comportamentos suspeitos nas infraestruturas do Contraente Público;
- f) UEBA – *User & Entity Behavior Analytics* – deteção de comportamentos anómalos ou improváveis dos colaboradores do Contraente Público;
- g) *Response and Automation* – dispor de funcionalidades de automação e fluxos pré-desenhados para conter ameaças e capacidade de integração com plataformas de ITSM para suporte a tickets junto de equipas operacionais do Contraente Público;
- h) *Incident Response and Investigations* – dispor de valências de correlação de informação sobre eventos com informação detalhada do mesmo por forma a permitir investigação imediata;
- i) Alinhamento com o *framework* MITRE ATT&CK, dispondo de biblioteca de métodos de ataques e deteção baseados neste *framework*.

12. Remediação de acordo com o definido em sede de implementação e procedimentos registados nos *playbooks*, ie, se há algum incidente de segurança nos *endpoints*, o adjudicatário tem de ser capaz de remediar o incidente de acordo com procedimentos acordados e não apenas disponibilizar ao adjudicante um manual de procedimentos para este executar a remediação.

13. Deve oferecer uma proteção da Identidade através da aplicação de políticas de proteção contra ameaças em tempo real, com *use cases* a demonstrar a capacidade de responder aos incidentes de forma automatizada.

14. Dispor de retenção de *Logs* por um período mínimo de 13 (treze) meses em *hot* (sempre disponíveis para acesso imediato) e disponibilidade de acesso e pesquisa durante esse período.

15. Contemplar mínimo de 3 (três) Campanhas de *Phishing* anuais para realizar ações de *Cyber Awareness*.

16. Contemplar no mínimo 5 (cinco) ações de *Threat Intelligence & Takedown* por ano.

17. Contemplar 1 *Pen Testing* anual com o máximo de 80 (oitenta) horas.

18. Dispor de *Dashboards* em tempo real para suporte à operação, permitindo acesso e visualização dos dados em tempo real com capacidade de os customizar de acordo com as necessidades da operação.

19. *Reporting* mensal respeitando os seguintes elementos informativos:

- a) Sumário Executivo – visão global da prestação dos serviços:
 - i. Gráficos de tendência:
 - 1. Incidentes de Segurança;
 - 2. Ameaças detetadas;
 - 3. Vulnerabilidades detetadas;
 - 4. Número de *takedowns*.
 - ii. Resumo dos Níveis de Serviço e taxa de sucesso.
- b) Gestão de inventário de segurança – dispor de indicadores dos *assets* geridos pelo serviço:
 - i. Visão dos estados dos *assets*:
 - 1. Número Total de *assets* geridos;
 - 2. Número Total de *assets* em conformidade;
 - 3. Número Total de *assets* em não conformidade, ou com alertas.
 - ii. Casos de *assets* que aguardam inputs do Contraente Público.
- c) Gestão de incidentes de segurança – dispor de indicadores de incidentes de segurança:
 - i. Número de Incidentes criados no mês;

- ii. Número de Incidentes resolvidos no mês;
 - iii. Número de Incidentes a aguardar resposta de Cliente;
 - iv. Número de Incidentes por Categoria baseado na Taxonomia ENISA (European Union Agency for Cybersecurity).
- d) Análise de vulnerabilidades – dispor de análises de vulnerabilidades realizadas e falhas detetadas:
- i. Vulnerabilidades Críticas;
 - ii. Top 10 de Servidores Vulneráveis;
 - iii. Top 10 Vulnerabilidades;
 - iv. Quantidade de Análises de Vulnerabilidades;
 - v. Calendário de Análises Vulnerabilidades para futuro.
- e) Análise de ameaças – dispor de informação do número de ameaças detetadas no mês:
- i. Ameaças detetadas na *Deep & Dark Web* e redes sociais, se aplicável;
 - ii. Domínios afetados pelas ameaças detetadas.
- f) *Takedown* – dispor de informação sobre *takedowns* realizados durante o mês e durante o ano:
- i. Informação relativa a *takedowns*, do site que estava a ser usado;
 - ii. Resumo da evolução de *takedowns* realizados nos últimos 12 (doze) meses.
- g) Campanhas de consciencialização – dispor de informação sobre a demonstração de estatísticas relativamente às campanhas realizadas:
- i. Número de utilizadores participantes na campanha;
 - ii. Número de Utilizadores que não abriram o email simulação;
 - iii. Número de Utilizadores que abriu o email simulação;
 - iv. Número de Utilizadores que carregou no url do email simulação;
 - v. Número de Utilizadores que participou como *Phishing* ou *Spam*.

20. Portal SOC, garantindo acesso às informações mais relevantes/impactantes do desempenho do serviço tais como:

- a) *Dashboard* Executivo com resumo de estatísticas de ameaças, benchmarking, gestão de ativos com eventos detetados e notícias relativamente a cibersegurança;
- b) Gestão de Incidentes de Segurança com acesso a estatísticas e a detalhes relativamente aos incidentes dos últimos 30 (trinta) dias, que poderão ser filtrados por categoria de incidente;
- c) Área de relatórios.

Cláusula 28.^a

Níveis de serviço

O Prestador de Serviços deve assegurar os seguintes níveis de serviço:

- a) Serviço a funcionar permanentemente 24x7x365, garantindo os seguintes tempos de resposta a incidentes:

Nível de Criticidade	Tempo de Resposta
Nível 1 – Crítico	30 minutos
Nível 2 – Alto	1 Hora
Nível 3 – Médio	2 Horas

b) Seguindo as regras de priorização abaixo apresentadas:

Categorias	Tipos de Incidentes	Nível de Prioridade
Código Malicioso (<i>Malware</i>)	Sistema Infetado	1
	Servidor C2	
	Distribuição de <i>Malware</i>	
	Configuração de <i>Malware</i>	
Tentativa de Intrusão	Exploração de Vulnerabilidade	1
	Tentativa de <i>login</i>	
	Nova assinatura de ataque	
Segurança da Informação	Acesso não autorizado	1
	Modificação não autorizada	
Disponibilidade	Negação de Serviço (DoS)	2
	Negação de Serviço Distribuída (DDoS)	
	Configuração incorreta	
Fraude	Utilização indevida ou não autorizada de recursos	3
	Direitos de autor	
	Utilização ilegítima de nome de terceiros	
	<i>Phishing</i>	
Intrusão	Compromisso de Conta Privilegiada	3
	Compromisso de Conta Não Privilegiada	
	Compromisso de Aplicação	
Recolha de Informação	<i>Scanning</i>	3
	<i>Sniffing</i>	
	Engenharia Social	
Vulnerabilidade		3
Conteúdo Abusivo		3
Outros	Outros incidentes de segurança	3

c) Incidentes com a mesma *root cause* são considerados como um único incidente para efeitos de apuramento.

Cláusula 29.^a

Forma de prestação dos serviços

1. A prestação decorrerá de acordo com o disposto no presente caderno de encargos e em coordenação com o gestor do contrato designado pelo Contraente Público.
2. Todos os relatórios, registos, comunicações, atas e demais documentos, elaborados pelo Prestador de Serviços para entregar ao Contraente Público, devem ser integralmente redigidos em português e elaborados em formato digital, e enviados por correio eletrónico ou por outro meio de transmissão eletrónica de dados a acordar entre as partes.
3. No final da execução do contrato, o Prestador de Serviços deve ainda elaborar um relatório final, discriminando os principais acontecimentos e atividades ocorridos em cada fase de execução do contrato.

Cláusula 30.ª

Aceitação dos serviços prestados

1. No prazo de 5 (cinco) dias a contar do fim da prestação dos elementos referentes a cada execução mensal do contrato, o Contraente Público procede à respetiva análise do serviço prestado, com vista a verificar se os mesmos reúnem as características, especificações e requisitos técnicos definidos nesta secção e na proposta adjudicada, bem como outros requisitos exigidos por lei.
2. Na análise a que se refere o número anterior, o Prestador de Serviços deve prestar ao Contraente Público toda a cooperação e todos os esclarecimentos necessários.
3. No caso de a análise do Contraente Público a que se refere o n.º 1 não comprovar a conformidade dos elementos prestados com as exigências legais, ou no caso de existirem discrepâncias com as características, especificações e requisitos técnicos definidos nesta secção, o Contraente Público deve disso informar, por escrito, o Prestador de Serviços.
4. No caso previsto no número anterior, o Prestador de Serviços deve proceder, à sua custa e no prazo razoável que for determinado pelo Contraente Público, às alterações e complementos necessários para garantir o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
5. Após a realização das alterações e complementos necessários pelo Prestador de Serviços, no prazo respetivo, o Contraente Público procede a nova análise, nos termos do n.º 1.
6. Caso a análise do Contraente Público a que se refere o n.º 1 comprove a conformidade dos elementos prestados pelo Prestador de Serviços com as exigências legais, e neles não sejam detetadas quaisquer discrepâncias com as características, especificações e requisitos técnicos definidos nesta secção, deve ser emitida, no prazo máximo de 2 (dois) dias a contar do termo dessa análise, declaração de aceitação pelo Contraente Público.
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 características, especificações e requisitos técnicos que se venham a detetar, previstos na presente secção.

Cláusula 31.ª

Garantia técnica

O Prestador de Serviços fica sujeito, com as devidas adaptações, às exigências legais, obrigações do fornecedor e prazos aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código dos Contratos Públicos, na sua redação atual, bem como toda a legislação e regulamentação portuguesa e europeia aplicável.