CONCURSO PÚBLICO INTERNACIONAL N.º 108/2025/DCP/DIT/

AQUISIÇÃO DE SERVIÇOS SECURITY OPERATIONS CENTER - SOC

Caderno de Encargos

CLÁUSULAS JURÍDICAS ____ **3**

Cláusula 1.ª Objeto ____ *3*

Cláusula 2.ª Local da prestação de serviços ____ *3*

Cláusula 3.ª Duração ____ *3*

Cláusula 4.ª Preço base global e preço base unitário ____ *3*

Cláusula 5.ª Condições de pagamento ____ *4*

Cláusula 6.ª Propriedade intelectual ____ *4*

Cláusula 7.ª Sigilo ____ *5*

Cláusula 8.ª Proteção de dados ____ *5*

Cláusula 9.ª Cessão da posição contratual e subcontratação ____ *7*

Cláusula 10.ª Comunicações e notificações ____ *7*

Cláusula 11.ª Penalidades contratuais ____ *7*

Cláusula 12.ª Retenção ____ *8*

Cláusula 13.ª Trabalhadores afetos à prestação de serviços ____ *8*

Cláusula 14.ª Foro competente ____ *8*

Cláusula 15.ª Legislação aplicável ____ *8*

CLÁUSULAS TÉCNICAS ____ **9**

Cláusula 16.ª Descrição técnica do contrato ____ *9*

Cláusula 17.ª Afetação de recursos, substituição e reforço das equipas ____ *13*

Cláusula 18.ª Perfil técnico dos recursos a afetar aos serviços ____ *13*

Cláusula 19.ª Níveis de serviço ____ *15*

Cláusula 20.ª Planeamento ____ *16*

Cláusula 21.ª Entregáveis e documentação ____ *16*

Cláusula 22.ª Gestor do Contrato ____ *16*

Cláusula 23.ª Requisitos específicos de implementação para a segurança da informação ____ *17*

Cláusula 24.ª Mecanismos formais de acompanhamento ____ *18*

CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

1. O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar com a Agência para a Modernização Administrativa, IP, (doravante abreviadamente designada por "AMA"), na sequência de procedimento pré-contratual que tem por objeto a aquisição de serviços de "Security Operations Center – SOC", nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.ª

Local da prestação de serviços

Os serviços serão prestados nas instalações do cocontratante.

Cláusula 3.ª

Duração

O contrato tem a duração de 10 meses contados do dia seguinte à data da sua celebração, ou até 30 de junho de 2026, conforme o que ocorrer primeiro, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preço base global e preço base unitário

1. O preço base global é de 261.353,90 €, a que acresce o IVA à taxa legal em vigor, para o período de 10 meses, o qual será consumido de acordo com o preço base unitário mensal de 26 135,39€, acrescido de IVA à taxa legal em vigor.

2. São excluídas as propostas cujo valor seja superior ao preço base apresentado na alínea anterior.

3. O preço referido no n.º 1 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à AMA, designadamente:

a) Despesas com deslocações, estadias e despesas de alimentação;

b) Encargos com telecomunicações;

c) Seguro de acidentes de trabalho.

4. Todos os encargos derivados da apresentação da proposta, assinatura do contrato, prestação de garantias e seguros são da responsabilidade do cocontratante, incluindo, caso o presente contrato seja submetido a fiscalização prévia e seja concedido o Visto, os emolumentos devidos ao Tribunal de Contas.

Cláusula 5.ª

Condições de pagamento

1. A faturação é efetuada mensalmente mediante a efetiva prestação dos serviços.
2. O pagamento será efetuado no prazo 30 dias a contar da data da receção da fatura correspondente, a qual só pode ser emitida após o vencimento da obrigação a que se refere.
3. A fatura deve discriminar o fornecimento a que se reporta, a referência do procedimento bem como o número de compromisso financeiro associado, o qual será indicado pela AMA, sob pena da sua devolução.
4. Caso a fatura apresentada não seja validada pela AMA, esta comunicará tal decisão ao cocontratante para que proceda à sua substituição.
5. As faturas deverão revestir a forma eletrónica, caso em que devem ser remetidos à AMA através de meio de transmissão escrita e eletrónica de dados para o Portal FEAP (Faturação Eletrónica na Administração Pública) disponibilizado pela ESPAP.
6. Só serão devidos os valores referentes aos serviços efetivamente prestados e aceites nos termos do presente caderno de encargos.
7. O pagamento será realizado para o NIB/IBAN indicado em documento bancário apresentado pelo cocontratante o qual deverá ser atualizado sempre que necessário.
8. Em caso de atraso no cumprimento das obrigações pecuniárias por parte da AMA, o cocontratante tem o direito aos juros de mora sobre o montante em dívida, nos termos previstos no artigo 326.º do CCP e da Lei n.º 3/2010, de 27 de abril.
9. Só são efetuados pagamentos após o pagamento dos emolumentos devidos ao Tribunal de Contas pela concessão do visto pelo cocontratante, nos termos do artigo 7.º do Decreto-Lei n.º 66/96, de 31 de maio, quando aplicável.

Cláusula 6.ª

Propriedade intelectual

1. Correm inteiramente por conta do cocontratante, os encargos e responsabilidades decorrentes da utilização, na execução do fornecimento de software ou de outros a que respeitem quaisquer patentes, licenças, marcas, desenhos registados e outros direitos de propriedade industrial ou direitos de autor ou conexos.
2. Se a AMA vier a ser demandada por ter sido infringido, na execução do contrato, qualquer dos direitos mencionados no ponto anterior, o cocontratante responderá nos termos do disposto no artigo 447.º, n.º 2, do Código dos Contratos Públicos.

Cláusula 7.ª

Sigilo

1. O cocontratante obriga-se a observar sigilo quanto a informação e documentação, técnica e não técnica, comercial ou outra, relacionada com a atividade da AMA ou qualquer outra entidade envolvida na execução do contrato.
2. A informação e documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. O cocontratante obriga-se ainda a respeitar a confidencialidade sobre todos os dados ou informações de carácter funcional ou processual dos serviços da Administração Pública a que tenha acesso na execução do contrato.
4. O cocontratante assume igualmente o compromisso de restituir, remover e destruir, no final do contrato, todo e qualquer registo, eletrónico ou em papel, relacionado com os dados e processos analisados, incluindo dados pessoais, e que a AMA lhe indique para esse efeito.
5. O cocontratante obriga-se, de um modo especial, a guardar sigilo quanto ao conteúdo e utilização dos sistemas de informação da responsabilidade da AMA, nos termos legalmente previstos, relativamente à proteção de dados pessoais e à proteção jurídica de bases de dados.
6. Após ter conhecimento de alguma violação de dados pessoais o cocontratante notifica a AMA sem demora injustificada, em prazo inferior a 48 horas.
7. O cocontratante garante que terceiros que envolva na execução dos serviços respeitem as obrigações de sigilo e confidencialidade constantes nos números anteriores.

Cláusula 8.ª

Proteção de dados

1. O Cocontratante é obrigado a tratar todos os dados pessoais a que tiver acesso, de acordo com o previsto no Regulamento Geral de Proteção de Dados Pessoais aprovado pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD), devendo, nomeadamente:
    a) Tratar os dados pessoais apenas mediante instruções documentadas da Entidade Adjudicante, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso a Entidade Adjudicante desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;
    b) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
    c) Adotar todas as medidas exigidas nos termos do artigo 32.º do RGPD;

d) Garantir o cumprimento do RGPD, nas condições aqui previstas, quando pretenda contratar um subcontratante;

e) Tomar em conta a natureza do tratamento, e na medida do possível, prestar assistência à Entidade Adjudicante pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos direitos previstos no capítulo III do RGPD;

f) Prestar assistência à Entidade Adjudicante no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e a informação ao seu dispor;

g) Consoante a escolha da Entidade Adjudicante, apagar ou devolver-lhe todos os dados pessoais depois de concluído o contrato, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros;

h) Disponibilizar à Entidade Adjudicante todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na presente cláusula, facilitando e contribuindo para as auditorias, inclusive as inspeções, conduzidas pela Entidade Adjudicante ou por outro auditor por esta mandatado.

2. A Entidade Adjudicante, no caso de suspeitar de incumprimento do RGPD, pode notificar o Cocontratante para este, no prazo de 5 dias, demonstrar o total cumprimento do referido regulamento.

3. Caso o Cocontratante não demonstre o total cumprimento do RGPD, seja porque não o demonstrou, seja porque não o cumpre, a Entidade Adjudicante fica autorizada a proceder à auditoria aos sistemas de informação do Cocontratante, ficando este responsável por todos os custos dessa auditoria.

4. No caso previsto no número anterior, a Entidade Adjudicante poderá compensar os custos que tenha suportado com eventuais quantias que sejam devidas ao Cocontratante, ou através do acionamento da caução, caso esta tenha sido prestada, ou através do recurso às retenções que eventualmente tenham sido efetuadas.

5. No caso de se verificar algum incumprimento do RGPD por parte do Cocontratante, este deverá, no prazo de 10 dias, por fim ao incumprimento e demonstrá-lo à Entidade Adjudicante.

6. O não cumprimento do RGPD, por facto imputável ao cocontratante, é considerado, para todos os efeitos, incumprimento definitivo, podendo a Entidade Adjudicante resolver o contrato, ao abrigo da alínea a) do n.º 1 do artigo 333.º do CCP.

7. Caso o Cocontratante impeça ou não colabore na realização da auditoria referida no n.º 3 da presente cláusula, a Entidade Adjudicante poderá resolver o contrato, por oposição reiterada ao exercício dos poderes de fiscalização, ao abrigo da alínea c) do n.º 1 do artigo 333.º do CCP.

Cláusula 9.ª

Cessão da posição contratual e subcontratação

1. O cocontratante não pode ceder a sua posição no contrato ou subcontratar total ou parcialmente os serviços incluídos no mesmo sem autorização prévia da AMA.
2. Nos casos de subcontratação, o cocontratante permanece integralmente responsável perante o contraente público pelo exato e pontual cumprimento de todas as obrigações contratuais.
3. A subcontratação de prestações contratuais que envolvam o tratamento de dados pessoais carece de autorização prévia da AMA que deverá ser realizada nos termos legalmente previstos para o efeito.
4. O cocontratante é responsável pelo tratamento de dados pessoais no âmbito da execução do contrato, mesmo que seja realizado por subcontratado.

Cláusula 10.ª

Comunicações e notificações

1. Sem prejuízo de se acordarem outras regras quanto às notificações e comunicações entre as partes, estas devem ser dirigidas para o domicílio ou sede contratual de cada uma nos termos previstos no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 11.ª

Penalidades contratuais

1. Pelo não cumprimento de obrigações emergentes do contrato, a AMA pode exigir do cocontratante o pagamento de uma sanção pecuniária, num montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
    a) Pelo incumprimento do prazo estipulado na alínea a) do nº 5 da cláusula 17ª pode ser aplicada uma penalidade de 100,00€ por cada dia de atraso.
    b) Pelo incumprimento dos níveis de serviço estipulados na cláusula 19ª:
        a. Disponibilidade mensal mínima indicada no nº 2 pode ser aplicada uma penalidade de 200,00€ por mês
        b. Tempos de resposta indicados no nº 3:
            i. Crítico – aplicada penalidade de 500,00€ por cada ocorrência
            ii. Alto – aplicada penalidade de 100,00€ por cada ocorrência
            iii. Baixo – aplicada penalidade de 50,00€ por cada ocorrência
    c) Pelo incumprimento dos prazos estipulados na cláusula 21.ª pode ser aplicada uma penalidade de 50,00€ por cada dia útil de atraso.
    d) Pelo incumprimento do prazo de implementação do serviço especificado no nº 1 da cláusula 20ª

pode ser aplicada uma penalidade de 150,00€ por cada semana de atraso.

e) Pelo incumprimento da disponibilização de relatórios mensais especificado na cláusula 21ª pode ser aplicada uma penalidade de 100,00€ por cada semana de atraso.

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

3. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida fatura no valor correspondente.

4. O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.

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

6. A aplicação das sanções previstas na presente cláusula será objeto de audiência prévia, nos termos previstos no n.º 2 do artigo 308.º do Código dos Contratos Públicos.

Cláusula 12.ª

Retenção

Quando não tenha sido exigida a prestação de caução, caso se revele pertinente, a AMA poderá proceder à retenção de 10% do valor dos pagamentos a efetuar, tendo em vista a garantia da perfeita e tempestiva execução do contrato, nos termos do disposto no n.º 3 do artigo 88.º do Código dos Contratos Públicos.

Cláusula 13.ª

Trabalhadores afetos à prestação de serviços

O cocontratante deve garantir, relativamente aos trabalhadores afetos à execução do contrato a celebrar, o cumprimento integral das disposições previstas no artigo 419.º-A do CCP.

Cláusula 14.ª

Foro competente

Para a resolução de todos os litígios relativos, designadamente, à interpretação, execução, incumprimento, invalidade, resolução ou redução do contrato é competente o Tribunal Administrativo de Círculo de Lisboa.

Cláusula 15.ª

Legislação aplicável

Em tudo o omisso neste Caderno de Encargos, observar-se-á o previsto no Código dos Contratos Públicos e demais legislação aplicável.

CLÁUSULAS TÉCNICAS

Cláusula 16.ª

Descrição técnica do contrato

Em outubro passado, a AMA enfrentou um ataque cibernético significativo que resultou na indisponibilidade dos seus sistemas e serviços públicos, afetando tanto cidadãos quanto empresas por vários dias. Este incidente destacou a vulnerabilidade dos sistemas da AMA e a necessidade urgente de implementar medidas de mitigação de risco para prevenir futuros ataques e minimizar os impactos de possíveis incidentes.

Uma das principais medidas definidas foi a constituição de um Centro de Operações de Segurança (SOC). A contratação de um serviço de SOC, baseado na plataforma de Gestão de Informações e Eventos de Segurança (SIEM) interna da AMA, é essencial para fortalecer a segurança cibernética da organização. Ressalva-se que o co-contratante poderá usar uma plataforma própria em complemento à da AMA.

O SOC desempenha um papel crucial na monitorização contínua dos sistemas de TI, identificando e respondendo a ameaças em tempo real. A plataforma de SIEM permite a coleta, análise e correlação de dados de segurança provenientes de diversas fontes, proporcionando uma visão abrangente e centralizada das atividades suspeitas e incidentes de segurança.

Ao implementar um SOC, a AMA beneficiará de:

- **Deteção Proativa de Ameaças**: O SOC permitirá a identificação precoce de atividades maliciosas, possibilitando uma resposta rápida antes que estas possam causar danos significativos.
- **Resposta Rápida a Incidentes**: Com uma equipa dedicada e ferramentas avançadas, o SOC pode responder de forma eficiente a incidentes de segurança, minimizando o tempo de inatividade e os impactos operacionais.
- **Análise e Relatórios Detalhados**: A plataforma de SIEM fornecerá relatórios detalhados sobre incidentes de segurança, ajudando a identificar padrões e tendências que podem ser usados para melhorar continuamente as defesas cibernéticas.
- **Conformidade e Auditoria**: O SOC ajudará a garantir que a AMA cumpre com as regulamentações e normas de segurança, facilitando auditorias e demonstrando o compromisso da organização com a segurança da informação.

Dada a gravidade do ataque cibernético sofrido e a crescente sofisticação das ameaças cibernéticas, a contratação de um serviço de SOC baseado na plataforma de SIEM interna da AMA é uma medida estratégica e necessária para proteger os sistemas e dados da organização, garantindo a continuidade dos serviços públicos e

a confiança dos cidadãos e empresas.

Os serviços de cibersegurança pretendidos visam fornecer uma solução de Security Operations Center (SOC), focada na cibersegurança contínua num modelo de serviços. Os requisitos focam-se numa abordagem que integra **redução de risco, prevenção ativa, e metodologias e tecnologias avançadas de deteção, resposta e mitigação de incidentes**, cobrindo toda a superfície de ataque.

Volumetrias de infraestruturas a cobrir pelo serviço:

- Número de Endpoints (PC desktop, PC portátil e tablets): 2700 Workstations
- Número de Servidores (AD, SQL, Windows, Linux, outros): 700 servidores incluindo servidores em Azure
- Número de Firewall e Web Application Firewall:
    a. Data Center 1:
        i. 2 WAFs (2 físicas em HA; e 2 no azure em HA);
        ii. 2 ADC (2 físicos em HA; dentro do HA estão 2 VDOMs);
        iii. 2 FW Checkpoint (2 físicas em HA; com 2 GWs);
        iv. 2 FW Fortinet (2 físicas em HA; uma tem 4 VDOMs, a outra tem 7 VDOMs)
    b. Data Center 2:
        i. 2 FW Fortinet (2 físicas em HA; com 4 VDOMs)
- Número de domínios públicos: 80
- Números IP públicos para publicação de sites/serviços: 170
- Números IP públicos para acessos à internet: 5
- Domínio Active Directory: 1 domínio
- Número de Sites: 150

Requisitos Gerais do Serviço SOC:

- **Serviço Contínuo e Abrangente**:
    - O serviço de cibersegurança deve ser **contínuo, operando 24x7x365**.
    - Deve cobrir toda a superfície de ataque, incluindo redes, TI, sites e a sensibilização dos colaboradores.
    - As tecnologias e equipas devem ser **de nova geração e altamente especializadas**.
    - O serviço deve ser prestado a partir de instalações localizadas em **território da União Europeia** e a equipa deve expressar-se em português.
    - As ferramentas SIEM/SOAR não devem ter limites de eventos nem de tráfego a ingerir, e o licenciamento deve ser responsabilidade do fornecedor.

COMPONENTES E FUNCIONALIDADES CHAVE DO SERVIÇO:

- **Gestão de Incidentes de Segurança**:
    - Monitorização contínua de equipamentos de TI através de **SIEM de nova geração**, com análise e classificação de eventos de segurança baseadas na **taxonomia ENISA**.
    - **Escalonamento claro e conciso** de incidentes de segurança para remediação.
    - **Automação de ações** para resolver ameaças de imediato.
    - Implementação de **automatismos de remediação** em *endpoints*, *firewalls* e *Active Directory*.
    - Suporte à **gestão de crise** para conter, mitigar e eliminar ataques, minimizando os seus efeitos.
    - Apoio às equipas do cliente nas fases de erradicação, recuperação e investigação de incidentes, incluindo contacto com entidades como o CNCS.
    - Registo e documentação de todas as ações efetuadas no tratamento de incidentes.
- **Gestão de Vulnerabilidades e Testes de Penetração**:
    - **Análise de vulnerabilidades** com pré-análise e deteção de potenciais vulnerabilidades na rede e sistemas de TI, com sugestão de correções e *timing* de implementação baseado na criticidade.
    - Utilização de *Light Agents* para recolha automática de dados em *endpoints* (Windows, Linux, Mac), mesmo em utilizadores remotos.
    - Prioritização de risco real e integração de projetos de remediação.
    - Avaliação de **infraestruturas *Cloud* e de virtualização**.
    - Redução da exposição ao risco de vulnerabilidades através de ações e configurações compensatórias (ex: NAC, *Firewalls*).
    - Realização de **testes de penetração (*Pen Testing*) anuais**, com duração máxima de 80 horas, em ambientes à escolha do cliente.
    - Testes de penetração devem ser realizados por equipas *Purple Team* (Red vs Blue).
    - Gestão de vulnerabilidades para **todos os ativos monitorizados** (ilimitado).
- **Inteligência de Ameaças e *Takedown***:
    - Análise contínua da **Deep & Dark Web**, redes sociais e domínios do cliente para deteção de informações corporativas expostas, venda de credenciais ou planos de ataque.
    - Serviço de *takedown* para assegurar a desativação de *websites* e domínios fraudulentos que simulam a marca do cliente (5 *takedowns* por ano).
    - Produção de IOC (Indicator of Compromise) e interligação com outras *feeds*.
    - Investigação forense (DFIR), com pelo menos 2 análises anuais.
    - Engenharia reversa de *malware*.
- **Sensibilização para a Cibersegurança (*Cyber Awareness*)**:
    - Campanhas periódicas de **simulação de *phishing*** (3 campanhas por ano)

- Avaliação de *e-mails* suspeitos através de tecnologia sem riscos.
- Utilização de uma plataforma completa para gestão de campanhas de simulação, fornecendo estatísticas de comportamento e sugerindo medidas corretivas.

- **Retenção de *Logs***:
  - Garantia da salvaguarda e retenção de *logs* por um período determinado (13 meses) para cumprimento legal e pesquisa imediata.
  - No final do contrato, os *logs* ingeridos devem poder ser exportados em formato *syslog* (ou outro padrão reconhecido) e entregues ao cliente.
- **Deceção (*Deception*)**:
  - Criação de armadilhas como *honeypots*, utilizadores fictícios e credenciais falsas para identificar comportamentos maliciosos no início da cadeia de ataque.
- **Análise Forense**: inclusão de análises forenses

METODOLOGIA E OPERACIONALIZAÇÃO:

- **Uso da matriz MITRE ATT&CK:** Utilização da framework MITRE para desenhar regras de eventos de segurança e definir casos de uso para automação.
- **Resposta a Incidentes e Investigações:** Informação correlacionada no próprio evento para investigação imediata.
- **Resposta e Automação:** Funcionalidades de automação e fluxos pré-desenhados para conter ameaças (ex: bloquear conta, isolar máquina), reduzindo trabalho manual repetitivo.
- **Ciclo de Vida de um Incidente:** O serviço acompanha o ciclo de vida do incidente desde a origem ao desfecho, com escalamento claro e notificações por e-mail e portal.

EQUIPAS ESPECIALIZADAS:

- ***Blue Team* (Centro de Resposta a Incidentes de Cibersegurança)**: Equipa responsável por lidar com as ameaças de forma contínua (24x7x365), com foco na resposta rápida, análise contínua de ativos expostos, elaboração de *playbooks* e *use cases*, e gestão de SIEM/SOAR.
- ***Purple Team* (Gestão de Ameaças)**: Equipa que define e realiza testes de penetração, explorando vulnerabilidades do ponto de vista de um atacante e promovendo contramedidas.
- ***Red Team***: Foca-se em detetar e explorar vulnerabilidades nas infraestruturas dos clientes, realizando testes de penetração e simulações de ataques direcionados.
- As equipas devem ser **dedicadas, qualificadas, experientes e certificadas** nas tecnologias utilizadas.

GOVERNANÇA, RISCO E CONFORMIDADE (*GRC*):

- Apoio na segurança da informação através de processos de melhoria contínua e campanhas de consciencialização.
- Apoio em auditorias, elaboração de *dashboards* e indicadores, validação de processos e documentação de segurança da informação.

Cláusula 17.ª

Afetação de recursos, substituição e reforço das equipas

1. Os recursos humanos a afetar à execução dos serviços referentes estão no âmbito de organização e sob a autoridade do cocontratante não existindo qualquer vínculo laboral com a AMA.
2. Durante a execução da prestação de serviços, a AMA poderá solicitar a substituição de algum dos elementos da Equipa, caso considere que este não reúne as condições necessárias ao desempenho das respetivas funções.
3. As férias ou outros impedimentos previsíveis por parte dos recursos afetos pelo prestador de serviços dá lugar à sua substituição.
4. Nas situações de substituição de recursos previstas nos números anteriores o cocontratante deverá submeter à aprovação da AMA o curriculum vitae do novo recurso, e garantir um período mínimo de dez dias úteis de transmissão de conhecimentos entre recursos.
5. Sempre que se constate a inadequação de algum elemento da equipa encarregue da execução dos serviços contratados, tendo em conta os requisitos exigidos e o comportamento comummente expectável, poderá a AMA exigir a sua substituição, aplicando-se, com as devidas adaptações, as seguintes regras.
    a) O cocontratante deverá, em 5 dias úteis, identificar o seu melhor recurso, e obter a aceitação da AMA;
    b) O cocontratante deverá assegurar que nos 5 dias úteis após a aceitação o recurso inicia a prestação do serviço.
6. O cocontratante deverá respeitar toda a legislação em vigor, na parte que lhe for aplicável, devendo, nomeadamente, observar as prescrições legais sobre a sanidade, salário mínimo, horários de trabalho, segurança e responsabilidade por acidentes de trabalho, sendo único responsável por quaisquer determinações ou sanções que lhe sejam impostas por entidades oficiais.
7. Findo o contrato, independentemente do fundamento da cessação, o destino do pessoal e as consequências emergentes dos contratos de trabalho são da responsabilidade do cocontratante.

Cláusula 18.ª

Perfil técnico dos recursos a afetar aos serviços

1. O Cocontratante deve indicar o perfil de qualificação proposto e a composição da equipa de suporte aos

serviços.

2. A equipa deve operar em território da União Europeia e expressar-se em português.
3. O cocontratante deve dispor de uma equipa multidisciplinar de, pelo menos, 4 (quatro) técnicos dedicados com o seguinte perfil:
    a) O coordenador da equipa deve possuir experiência mínima de 5 (cinco) anos na área de Cibersegurança;
    b) Os elementos técnicos a afetar à prestação dos serviços SOC devem possuir, individualmente, experiência mínima de 3 (três) anos na área de Cibersegurança;
    c) Os elementos técnicos têm de possuir individualmente, pelo menos, 2 (duas) das seguintes certificações:
        i. CISSP – Certified Information Systems Security Professional
        ii. CISM – Certified Information Security Manager;
        iii. (CISA) Certified Information Systems Auditor
        iv. GIAC Security Operations Manager
        v. CEH - Certified Ethical Hacker
        vi. CHFI - Computer Hacking Forensic Investigator
        vii. CompTIA Security+
        viii. CompTIA CySA+
        ix. CompTIA Analyst+
        x. CompTIA Pentest+
        xi. ISO IEC 27001
        xii. GCIH-Certified Incident Handler
        xiii. CSA – Certified SOC Analyst
        xiv. CCSA - Certified Cybersecurity Analyst
        xv. Information Security Foundation (ISFS) – EXIN
        xvi. CND – Certified Network Defender
        xvii. OSCP – Offensive Security Certified Professional
        xviii. GCFA - SANS FOR508 - Advanced Incident Response, Threat Hunting and Digital Forensics
        xix. GCIA -Network Intrusion Analyst
        xx. GIAC Certified Forensic Analyst;
        xxi. CSIE - CompTIA Secure Infrastructure Expert
        xxii. IAAP Certified Information Privacy Professional / Europe (CIPP/E)
        xxiii. Blue Team Level 1 (BTL1)
        xxiv. NSE 7 – Network Security Aschitect
        xxv. Fortinet – Certified Professional – ou equivalente

d) Cumulativamente, a equipa deverá possuir no mínimo, 6 (seis) das certificações indicadas na alínea c) da presente cláusula.

Cláusula 19.ª

Níveis de serviço

1. Para efeitos de contabilização de prazos, são tidos em conta todos os dias do ano.
2. O serviço deve operar 24x7x365, com uma disponibilidade mensal mínima de 99,99% para o SOC.
3. Matriz de níveis de serviço e prioridades:

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

Notas:

- Incidentes com a mesma causa-raiz (*root cause*) são considerados um único incidente.
- O mapeamento das prioridades poderá ser revisto e acordado durante a fase de implementação

Nível de Criticidade	Tempo de Resposta
Nível 1 – Crítico	**30 minutos**
Nível 2 – Alto	**1 hora**
Nível 3 – Médio	**2 horas**

Cláusula 20.ª

Planeamento

1. O serviço deverá ficar implementado e operacional num prazo máximo de 2 (dois) meses contados da data da assinatura do contrato.
2. A implementação do serviço será dividida em fases (Preparação, Implementação e Go-Live), seguindo metodologias de gestão de projeto (ex: PMBook® Guide do PMI):
    a) A fase de pré-implementação inclui desenho e revisão do setup da solução, preparação da infraestrutura, modelo de ameaças e gap analysis, e análise de ameaças na Deep & Dark Web.
    b) A fase de implementação inclui conectividades e permissões, deployment de light agents, configuração de regras SIEM, criação de Use Cases em SOAR e fine tuning.
    c) O Go-Live da solução requer validação formal do cliente.
3. Devem ser definidos um plano de comunicação e reuniões periódicas (semanais, quinzenais, mensais) em articulação entre a AMA e o Cocontratante de acordo com o estipulado na clausula seguinte.

Cláusula 21.ª

Entregáveis e documentação

1. A comunicação entre a AMA e o cocontratante no âmbito deste serviço deve ser suportada por uma ferramenta colaborativa (aplicação web) ou por email, tendo de disponibilizar obrigatoriamente a seguinte informação:
    a) Relatórios mensais ou com cadência alinhada entre as partes e
    b) Os relatórios devem incluir sumários executivos, gráficos de tendência (incidentes, ameaças, vulnerabilidades, *takedowns*), resumo de níveis de serviço, gestão de inventário de segurança, estatísticas de deceção, análise de vulnerabilidades, análise de ameaças e estatísticas de campanhas de *phishing*.
    c) Um **Portal de Serviço** deve permitir aos clientes acompanhar a prestação do serviço de forma autónoma (incidentes ativos, estatísticas, *takedowns*, remediações automáticas, inventário de ativos, análises de vulnerabilidades, repositório de relatórios).
    d) Manutenção de inventário de ativos na plataforma SIEM.

Cláusula 22.ª

Gestor do Contrato

1. O gestor do contrato, com a função de acompanhar permanentemente a execução contratual, nos termos e para os efeitos previstos no artigo 290.º-A do CCP, será designado pela AMA no contrato.

2. O cocontratante deverá indicar a pessoa na sua organização que será responsável pela execução do contrato, e que será o interlocutor com o gestor do contrato designado pela AMA, bem como a pessoa responsável pelo tratamento de dados pessoais.
3. No âmbito do presente contrato, a AMA, através do gestor do contrato designado nos termos do número 1., procederá à avaliação do cocontratante, de acordo com a matriz de avaliação de que se encontra disponibilizada no site institucional da AMA, em: https://www.ama.gov.pt/.

Cláusula 23.ª

Requisitos específicos de implementação para a segurança da informação

1. No decorrer da execução do contrato o fornecedor obriga-se a cumprir as políticas e procedimentos do SGSI sempre que estes se apliquem.
2. Cumprir o Procedimentos de desenvolvimento seguro englobado no SGSI, incluindo:
   a) Na definição de requisitos incluir os requisitos de segurança e privacidade;
   b) Não utilização de bibliotecas de terceiros sem prévia validação da AMA;
   c) Revisão de código por outro membro da equipa de desenvolvimento outra equipa do fornecedor, antes da passagem da aplicação para testes;
   d) Executar análise dinâmica à aplicação para verificação de problemas relativos a segurança;
   e) Relatório de PDS com informação sobre componentes de segurança e cumprimento do procedimento de desenvolvimento seguro;
   f) Relatório de testes à aplicação com inclusão dos testes relativos à componente de segurança antes da passagem a qualidade/produção.
3. O equipamento usado pelos consultores externos tem o Sistema Operativo atualizado, estão protegidos com sistemas antivírus e são regularmente verificados pelo fornecedor quanto à presença de malware.
4. Os equipamentos dos fornecedores que contenham informação da AMA de nível superior a público devem estar encriptados para proteção da informação em caso de perda ou roubo do equipamento.
5. O fornecedor fica sujeito a política de Gestão de fornecedores.
6. Os fornecedores só terão acesso à informação necessária para execução do projeto após esta ser disponibilizada pela AMA. O acesso à informação, nomeadamente ao código fonte, será dado mediante abertura de acessos individuais ao consultor, após efetuado o respetivo pedido pelo GP junto da DIT.
7. O fornecedor não pode negar uma auditoria relativamente às condições de desenvolvimento do projeto por parte dos seus consultores, caso esta seja requerida pela AMA.
8. Todos os consultores são obrigados a reportar qualquer incidente de segurança de informação que esteja relacionada com informação da AMA, de acordo com o Procedimento PR-005 Procedimento de Gestão de Incidentes.

9. No caso de ser um produto alojado em Cloud é obrigatório que conste da proposta apresentada, o local ou locais onde a informação possa ficar alojada e quais as certificações de segurança nacionais e internacionais que o local (físico e lógico) possui.

Cláusula 24.ª

Mecanismos formais de acompanhamento

1. A estrutura de coordenação da AMA é liderada pela Equipa de Comunicações e Segurança da Direção de Sistemas de Informação, a qual será assessorada pela equipa de especialistas/técnicos de informática da AMA (nas suas diversas valências) que assegurarão a avaliação da qualidade dos serviços prestados, da documentação e entregáveis disponibilizadas pelo cocontratante.

2. Para o acompanhamento da execução do contrato, o cocontratante fica obrigado a manter reuniões de progresso, com uma periodicidade mensal.

3. As reuniões previstas no número anterior devem ser alvo de uma convocação escrita por parte da AMA ou do cocontratante, com indicação dos assuntos a serem tratados.

4. O cocontratante fica obrigado a apresentar à AMA os relatórios previstos nas Cláusulas Técnicas do presente Caderno de Encargos, com a periodicidade aí definida.

5. Sem prejuízo de outros dados indicados nas Cláusulas Técnicas do presente Caderno de Encargos, os relatórios de níveis de serviço, referidos no número anterior da presente cláusula, devem incluir os seguintes dados:

a) Identificação da entidade adquirente;
b) N.º de Contrato;
c) Duração prevista do Contrato;
d) Informação relativa aos prazos, cumprimento de datas para a disponibilização dos serviços contratados, bem como a sua disponibilidade mensal;
e) Informação sobre incumprimentos relativos à prestação dos serviços, tipos de serviços afetados e respetiva justificação;
f) Informação relativa ao tipo e qualidade do serviço de apoio prestado;
g) Tipo e quantidade de serviços prestados sem a qualidade requerida;
h) Sanções aplicadas pela AMA e respetiva motivação.

6. Os relatórios previstos no número 4. da presente Cláusula deverão ser disponibilizados à AMA, pela forma que vier a ser acordada, até ao dia que antecede a reunião mensal de progresso, do período a que respeita.

7. O cocontratante envia à AMA, por correio eletrónico, com uma periodicidade mensal, até ao vigésimo dia do mês subsequente ao mês a que dizem respeito, relatórios de faturação.

8. Os relatórios de faturação devem conter os seguintes elementos:

a) Identificação da entidade adquirente;
b) N.º de Contrato;
c) Duração prevista do Contrato;
d) Datas de início e de fim do Contrato;
e) Descrição dos serviços prestados;
f) Valor faturado;
g) Valor de Contrato.

9. Todos os relatórios, registos, comunicações, atas e demais documentos elaborados pelo cocontratante devem ser integralmente redigidos em língua portuguesa.