



CADERNO DE ENCARGOS

OBJETO CONTRATUAL: PRESTAÇÃO DE SERVIÇOS DE CAPACITAÇÃO DOS SMAS DA MAIA PARA CUMPRIMENTO DOS REQUISITOS DE SEGURANÇA E RESPOSTA A INCIDENTES INFORMÁTICOS - CIBERSEGURANÇA - PELO PRAZO DE 1 ANO

PREÇO BASE DO PROCEDIMENTO: 29.000,00€ (VINTE E NOVE MIL EUROS)

PROCEDIMENTO: CONSULTA PRÉVIA, AO ABRIGO DA ALÍNEA C), DO N.º 1 DO ARTIGO 20.º, DO CÓDIGO DOS CONTRATOS PÚBLICOS, NA SUA REDAÇÃO ATUAL

FEVEREIRO 2022

SERVIÇOS MUNICIPALIZADOS DE ÁGUA E SANEAMENTO DA MAIA

PRESTAÇÃO DE SERVIÇOS DE CAPACITAÇÃO DOS SMAS DA MAIA PARA CUMPRIMENTO DOS REQUISITOS DE SEGURANÇA E RESPOSTA A INCIDENTES INFORMÁTICOS - CIBERSEGURANÇA

ÍNDICE

1 - CLÁUSULAS GERAIS.....	3
Cláusula 1ª – Objeto.....	3
Cláusula 2ª – Contrato.....	3
Cláusula 3ª – Prazo de execução do contrato.....	3
Cláusula 4ª – Obrigações do prestador do serviço.....	4
Cláusula 5ª – Conformidade e garantia técnica.....	4
Cláusula 6ª – Gestor do Contrato.....	4
Cláusula 7ª – Condições de pagamento.....	4
Cláusula 8ª – Resolução por parte da entidade adjudicante.....	5
Cláusula 9ª – Resolução por parte do prestador do serviço.....	5
Cláusula 10ª – Resolução de litígios.....	5
Cláusula 11ª – Subcontratação e cessão da posição contratual.....	5
Cláusula 12ª – Comunicações e notificações.....	5
Cláusula 13ª – Contagem de prazos.....	6
Cláusula 14ª – Avaliação de Desempenho.....	6
Cláusula 15ª – Dever de Sigilo.....	6
Cláusula 16ª – Proteção de Dados.....	6
Cláusula 17ª – Legislação aplicável.....	7
2 – CLÁUSULAS ESPECIAIS.....	8
Cláusula 18ª – Enquadramento e âmbito da prestação de serviços.....	8
Cláusula 19ª – Faseamento de atividades.....	9
Cláusula 20ª – Prazo de execução.....	17
Cláusula 22ª – Obrigações dos SMAS da Maia.....	17

1 - CLÁUSULAS GERAIS

Cláusula 1ª – Objeto

O contrato a celebrar tem por objeto a “**Prestação de Serviços de Capacitação dos SMAS da Maia para Cumprimento dos Requisitos de Segurança e Resposta a Incidentes Informáticos - Cibersegurança**”, pelo prazo de 1 ano.

Cláusula 2ª – Contrato

- 1 - O contrato será constituído pelo respetivo clausulado contratual e seus anexos, se aplicável.
- 2 - O contrato integra ainda os elementos seguintes:
 - a) Os suprimientos dos erros e das omissões ao Caderno de Encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c) O presente Caderno de Encargos;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos prestados pelo adjudicatário sobre a sua proposta.
- 3 - Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem que aí são indicados.
- 4 - Em caso de divergência entre os documentos referidos no ponto anterior e o clausulado do contrato, prevalecem os primeiros, pela ordem pela qual aí são indicados, salvo quanto aos ajustamentos propostos de acordo com o disposto no art.º 99.º, do CCP e aceites pelo adjudicatário, nos termos do art.º 101.º, do CCP.

Cláusula 3ª – Prazo de execução do contrato

A prestação do serviço deverá ser realizada no prazo de **1 ano** contados da data de publicitação do contrato escrito no Portal dos Contratos Públicos, www.basegov.pt.

Cláusula 4ª – Obrigações do prestador do serviço

Sem prejuízo das obrigações constantes no capítulo V – Aquisição de Serviços, do Título II - Contratos Administrativos em Especial, da Parte III – Regime Substantivo dos Contratos Administrativos, do C.C.P., o prestador de serviços compromete-se a dar atendimento adequado à satisfação das necessidades do adjudicante, no que diz respeito à prestação de todos os serviços que se encontram no âmbito deste procedimento.

Cláusula 5ª – Conformidade e garantia técnica

A prestação do serviço fica sujeita às exigências, prazos de garantia e demais obrigações legais, aplicáveis no âmbito de um contrato de prestação de serviços, nos termos do disposto no CCP bem como de outra legislação aplicável.

Cláusula 6ª – Gestor do Contrato

- 1 - O Conselho de Administração dos SMAS da Maia nomeará o Gestor do Contrato que terá como função o acompanhamento permanente da execução do mesmo.
- 2 - Sempre que se verifiquem desvios, defeitos ou outras anomalias na execução do contrato, o Gestor do Contrato terá de comunica-los, de imediato, ao Conselho de Administração dos SMAS da Maia, propondo em relatório fundamentado, as medidas corretivas que em cada caso se revelem adequadas.

Cláusula 7ª – Condições de pagamento

- 1 - A quantia devida pela entidade adjudicante deve ser paga após a receção da respetiva fatura, a qual só poderá ser emitida após o vencimento da respetiva obrigação.
- 2 - A faturação a emitir deverá exibir o **n.º da Proposta de Cabimento** e o **n.º do Compromisso** respetivo, cujas referências constarão nos documentos inerentes à Adjudicação, em cumprimento da legislação aplicável.
- 3 - Se a fatura não exibir o **n.º da Proposta de Cabimento** e o **n.º do Compromisso**, bem como da data de vencimento (30 dias), será devolvida para efeito de correção.

Cláusula 8ª – Resolução por parte da entidade adjudicante

- 1 - Sem prejuízo de outros fundamentos de resolução do contrato previstos na Lei, a entidade adjudicante pode resolver o contrato, a título sancionatório, no caso de o prestador do serviço violar, de forma grave ou reiterada, qualquer das obrigações que lhe incumbem.
- 2 - O direito de resolução referido no número anterior exerce-se mediante simples declaração enviada ao adjudicatário.

Cláusula 9ª – Resolução por parte do prestador do serviço

- 1 - Sem prejuízo de outros fundamentos de resolução previstos na Lei, o prestador do serviço pode resolver o contrato quando qualquer montante que lhe seja devido esteja em dívida há mais de 90 dias ou o montante em dívida exceda 25% do preço contratual.
- 2 - O direito de resolução é exercido por via judicial, com exceção da situação descrita no número anterior, em que poderá ser exercido mediante declaração ao contraente público, aplicando-se o disposto no n.º 4), do art.º 332.º, do Código dos Contratos Públicos.

Cláusula 10ª – Resolução de litígios

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

Cláusula 11ª – Subcontratação e cessão da posição contratual

A subcontratação pelo prestador do serviço e a cessão da posição contratual de qualquer das partes rege-se pelo disposto no Código dos Contratos Públicos.

Cláusula 12ª – Comunicações e notificações

- 1 - Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas para o domicílio ou sede contratual de cada uma, conforme disposto no Código dos Contratos Públicos
- 2 - Qualquer alteração deve ser comunicada por escrito à outra parte.

Cláusula 13ª – Contagem de prazos

- 1 - Os prazos previstos para a formação do contrato contam-se de acordo com o disposto no art.º 470.º do Código dos Contratos Públicos.
- 2 - Os prazos previstos para a execução do contrato contam-se de acordo com o disposto no art.º 471.º do Código dos Contratos Públicos.

Cláusula 14ª – Avaliação de Desempenho

- 1 - O prestador do serviço fica sujeito a uma avaliação de desempenho no âmbito da Certificação do Sistema de Gestão da Qualidade dos Serviços Municipalizados da Maia, por forma a ser dado cumprimento ao especificado no referencial normativo NP EN ISO 9001:2015.
- 2 - O prestador do serviço é avaliado com base nos critérios seguintes: ***Qualidade, Prazos, Segurança, Ambiente e Disponibilidade.***

Cláusula 15ª – Dever de Sigilo

- 1 - O prestador do serviço deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante, de que tenha conhecimento em virtude da execução do contrato.
- 2 - A informação e documentação abrangidas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento, que não o destinado direta e exclusivamente à execução do contrato.
- 3 - Exclui-se do dever de sigilo a informação ou documentação que seja comprovadamente do domínio público ou que este seja legalmente obrigado a revelar, por força da Lei ou de processo judicial.

Cláusula 16ª – Proteção de Dados

- 1 - O prestador do serviço, na qualidade de “entidade subcontratante” dos SMAS da Maia, sujeita-se ao cumprimento de todas as obrigações que sobre si recaem, nos termos da legislação em vigor em Portugal em matéria de privacidade e proteção de dados, nomeadamente a Lei n.º 67/98, de 26 de outubro e o Regulamento Geral de Proteção de Dados, Regulamento (UE) 2016/679, de 27 de abril de 2016, na execução de todas e quaisquer operações de tratamento de dados pessoais que deva levar a cabo no âmbito da prestação do serviço objeto do presente Contrato e exclusivamente no âmbito do mesmo.

- 2 - O prestador do serviço declara que não existe qualquer motivo que o impeça de cumprir escrupulosamente o estabelecido no número anterior e obriga-se:
 - a) A comunicar de forma detalhada aos SMAS da Maia qualquer circunstância que ocorra, durante a vigência do presente contrato, que o impeça de cumprir essas obrigações;
 - b) A disponibilizar aos SMAS da Maia todas as informações necessárias para demonstrar o cumprimento da legislação referida no número anterior.
- 3 - Os dados pessoais serão tratados pelo prestador do serviço em estrito cumprimento das instruções estabelecidas pelos SMAS da Maia, as quais poderão ser alteradas por estes, mediante envio ao prestador do serviço, por correio eletrónico ou qualquer outro meio, de documento escrito com as instruções atualizadas e a data da produção de efeitos.
- 4 - O prestador do serviço obriga-se a não transmitir os dados pessoais a terceiros, salvo se a transmissão for imposta por legislação vigente ou for consentida previamente pelos SMAS da Maia.
- 5 - O objeto de tratamento de dados traduz-se em obter conhecimento da identificação de trabalhadores.
- 6 - Os dados pessoais transmitidos ao prestador do serviço deverão ser eliminados por este no final da vigência do presente contrato.
- 7 - Os SMAS da Maia cumprirão, ainda, as obrigações que lhe caibam nos termos da legislação em vigor.

Cláusula 17ª – Legislação aplicável

O contrato é regulado pela legislação portuguesa.

2 – CLÁUSULAS ESPECIAIS

Cláusula 18ª – Enquadramento e âmbito da prestação de serviços

- 1 - A prestação de serviços objeto do contrato visa a capacitação dos SMAS da Maia, enquanto operador de serviço essencial, para dar cumprimento ao Regime Jurídico da Segurança do Ciberespaço, aprovado pela Lei nº 46/2018, de 13 de agosto, entretanto regulamentada pelo Decreto-Lei nº 65/2021, de 30 de Julho, nomeadamente:
 - a) Aos requisitos de segurança das redes e dos sistemas de informação nos termos dos artigos 12.º, 14.º e 16.º do Regime Jurídico da Segurança do Ciberespaço;
 - b) Aos requisitos de notificação de incidentes que afetem a segurança das redes e dos sistemas de informação nos termos dos artigos 13.º, 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço, prevendo as circunstâncias, o prazo, o formato e os procedimentos aplicáveis.
- 2 - Desta forma, pretende-se gerir, controlar, monitorizar, mitigar e reportar Incidentes de Segurança Informáticos, no sentido de dotar os SMAS DA MAIA de capacidade de resposta a este tipo de situações. Esta capacidade de resposta deverá ainda fornecerá recursos de segurança essenciais para maximizar a visibilidade de segurança e gestão de conformidade, nomeadamente a identificação de ativos, a avaliação e análise de vulnerabilidades, a correlação de logs/eventos (SIEM - Security information and event management), resposta a incidentes, análise de risco, gestão de logs, relatórios de compliance (SOX, ISO27001, RGPD,...), alertas por email, ticketing integrado / alertas, monitorização comportamental, análise forense, monitorização dark web e MSS (Managed Security Services). O prestador de serviços manterá estes recursos ativos e atualizados contra as últimas vulnerabilidades, com atualização contínua de inteligência face a novas ameaças, num formato 24x7, durante o período de execução do contrato.

Cláusula 19ª – Faseamento de atividades

A presente prestação de serviços inclui as fases a seguir definidas:

1. Fase 1 – Diagnóstico segundo ISO 27001:2013 e ISO 27005

1.1 O diagnóstico deve ser elaborado com base nos seguintes requisitos/controles da norma:

- A.5 – Política de Segurança
- A.6 – Organização da Segurança da informação
- A.7 – Segurança dos Recursos Humanos;
- A.8 - Gestão de Ativos;
- A.9 – Controlo de Acessos;
- A.10 – Criptografia;
- A.11 – Segurança física e ambiental;
- A.12 – Segurança das operações;
- A.13 – Segurança de Comunicações;
- A.14 – Aquisição, desenvolvimento e manutenção de sistemas;
- A.15 – Relações com fornecedores;
- A.16 – Gestão de incidentes de segurança da informação;
- A.17 – Aspetos da segurança da informação na gestão da continuidade do negócio;
- A.18 – Conformidade.

1.2 O diagnóstico referido no ponto anterior servirá para o prestador de serviços:

- a) Identificar o Responsável de Segurança;
- b) Identificar funções e atividades críticas;
- c) Estabelecer canais de comunicação;
- d) Análise de risco;
- e) Cadeia de responsabilidade;
- f) Política de Segurança;
- g) Procedimento de notificação de incidentes;
- h) Recolha das configurações de switching e routing (layer 2 e 3) para análise das metodologias de segurança utilizadas.

1.3 Durante esta fase, compete ao prestador de serviços executar as seguintes atividades:

- a) Definição da cadeia de responsabilidade;
- b) Definição dos privilégios de acesso individual, tendo em contas funções desempenhadas e as responsabilidades inerentes;
- c) Criação da política de segurança de informação adequada à organização, atendendo às suas necessidades e responsabilidades;
- d) Elaboração de um procedimento de notificação de incidente de cibersegurança, com impacto nas funções ou atividades identificadas como críticas;
- e) Resultado da análise de conformidade com a legislação aplicável e normas da área de atividade;
- f) Criação de uma política de uso aceitável - PUA;
- g) Elaboração de um plano de segurança contendo a política de segurança, descrição das medidas organizativas.

2. Fase 2 – PTES

2.1 O PTES (Penetration Testing Execution Standard) conjugado com o ISO 27001:2013 terá os pressupostos de base seguintes:

- a) Pré-engagement interactions;
- b) Intelligence Gathering;
- c) Threat Modeling;
- d) Vulnerability Analysis;
- e) Exploitation;
- f) Post Exploitation;
- g) Reporting.
- h) Avaliação das propriedades ACID (Atomicidade, Consistência, Isolamento e Durabilidade);
- i) Testes de benchmark TPC-C(l)
- j) Avaliar o modelo de dados (sql schema);
- k) Avaliar a framework aplicacional.

2.2 Desta fase devem resultar as seguintes informações:

- a) Tecnologias, sistema (configurações e fabricantes), recursos humanos;
- b) Arquitetura de rede e sistemas instalados/em operação;
- c) Arquitetura aplicacional, frameworks e BD's;
- d) Desenhos de base de dados, das aplicações e arquitetura de comunicação, níveis de acessos e interligações;
- e) Coordenação da injeção de incidentes (ataques DoS, RFI/LFI, Fuzzing) com a equipa de IT;
- f) Identificação do IP público a partir do qual serão injetados incidentes de segurança.

2.3 Durante esta fase, compete ao prestador de serviços entregar:

- a) Desenho e Implementação da arquitetura e segurança perimétrica
- b) Elaboração e/ou atualização do inventário de ativos;
- c) Criação de mecanismos proporcionais ao risco existente de eliminação ou corrupção de dados em sistemas que são importantes para o bom funcionamento da organização;
- d) Auditorias de segurança às bases de dados da organização;
- e) Realização de robustecimento dos sistemas, alinhado com o mapeamento das ameaças, ações de mitigação dos riscos e com a execução das atividades corretivas.

3. Fase 3 – Resposta a incidentes

3.1 O desenvolvimento desta fase assenta:

- a) Setup SIEM - Security Information and Event Management ;
- b) Tunning dos sensores;
- c) Mapeamento de rede/vulnerability scanning;
- d) Monitorização em tempo real e análise da triagem/incidente;
- e) Vulnerability Analysis coletar, reter e armazenar dados de auditoria/criação e gestão de conteúdos de auditoria;
- f) Implementação de contramedidas;
- g) Resposta a incidentes no local;
- h) Ferramentas de engenharia.

3.2 A análise dos aspetos elencados no ponto anterior servirá para o prestador de serviços:

- a) Verificar a recolha de informação de registo (logs) e período de armazenamento dos mesmos, providenciando a monitorização aos portais;
- b) Recolher informação sobre a arquitetura e tecnologias utilizadas em toda a estrutura IT com principal ênfase na DMZ;
- c) Identificar e analisar os ativos da rede;
- d) Identificar os servidores (independentemente do sistema operativo) para verificação de GPO's, portas/protocolos e serviços disponibilizados.

3.3 Durante esta fase, compete ao prestador de serviços executar as seguintes ações:

- a) Implementação de um sistema de recolha do fluxo de tráfego;
- b) Implementação de um procedimento de comunicação entre a organização e o Centro Nacional de Cibersegurança;
- c) Criação de instrumentos de correção ou mitigação de incidentes, atualização de ativos, triagem, análise de observáveis, fluxo de informação interno e de interação com entidades externas;
- d) Instalação e configuração de um sistema de monitorização
- e) Apoio ao sistema de gestão e correlação de dados e eventos, por forma a facilitar a análise em tempo real e acelerando a tomada de ações defensivas;
- f) Realização de dois simulacros de incidente de cibersegurança para avaliação da organização.

4. Fase 4 – Formação

4.1 Compete ao prestador de serviços ministrar aos colaboradores dos SMAS da Maia as formações/Sensibilização relativas aos módulos seguintes:

- a) Introdução à Segurança da Informação - Explicar a importância da segurança no contexto do dia-a-dia do colaborador.
- b) Introdução ao phishing - Fornecer uma visão breve mas concisa, das práticas recomendadas relacionadas à identificação e tratamento de emails suspeitos.

- c) Evitar links perigosos – Fornecer aos colaboradores orientações práticas sobre como descobrir o destino real de um URL e examinar dicas visuais comuns que podem ajudar os colaboradores a determinar se um site é legítimo ou perigoso.
- d) Evitar anexos perigosos - Ajudar os colaboradores a entenderem por que devem tratar qualquer anexo de email com uma suspeita saudável e como lidar com este tipo de conteúdos.
- e) Phishing de entrada de dados - Explicar os perigos associados a formulários de entrada de dados maliciosos e ajudar os colaboradores a entenderem por que eles devem ser cautelosos com qualquer email que inclua uma solicitação de credenciais ou outras informações confidenciais.
- f) Ferramentas de proteção de email - Entender como proteger-se contra ataques de phishing em combinação com ferramentas de proteção do serviço de email.
- g) Segurança do email em dispositivos móveis - Identificar e evitar emails de phishing em dispositivos móveis.
- h) Ameaças de spear phishing - Reconhecer e evitar ataques de phishing direcionados.
- i) Fundamentos de Segurança - Formar sobre os fundamentos da segurança informática, com vista a que o colaborador perceba as ameaças e erros mais comuns na vida diária.
- j) Fundamentos de segurança em trabalho remoto - Reconhecer e evitar ameaças encontradas no trabalho realizado remotamente.
- k) Formação de URL – os colaboradores aprendem como examinar um URL, entender a origem do link e identificar URLs fraudulentos ou mal-intencionados.
- l) Segurança do email - Detetar técnicas de phishing em emails e reconhecer links, anexos e informações falsificados.
- m) Segurança da Password – Ensinar técnica de criação de passwords mais fortes, usar uma família de passwords para ajudar na recuperação da password e guardar passwords com segurança.
- n) Redes Sociais Seguras – Educar os colaboradores sobre tipos de “fraudes” que podem ser encontrados nos sites sociais, implicações

das redes sociais com informação demasiado exposta e como detetar mensagens fraudulentas nas redes sociais.

- o) Proteger contra o Ransomware - Breve módulo de formação sobre como reconhecer e prevenir ataques de ransomware.
- p) Segurança de aplicações para dispositivos móveis - aprender a pesquisar componentes de aplicações e as implicações de permissões perigosas, que podem ajudá-los a avaliar a confiabilidade e a segurança das aplicações móveis antes de efetuarem download.
- q) Segurança de dispositivos USB – Sensibilizar para as ameaças frequentemente negligenciada, nomeadamente os riscos associados às unidades USB e de outros equipamentos IoT alimentados por meio de portas USB.
- r) Segurança física - Aprender como evitar e corrigir violações de segurança física e obter as práticas recomendadas que ajudarão a manter pessoas, áreas e ativos seguros.
- s) Segurança além do escritório - educar os colaboradores a usar o Wi-Fi gratuito com segurança, os riscos do uso de computadores públicos e as proteções para equipamentos e informações da organização em casa e em viagem.
- t) Navegação segura na Web – Compreender a diferença entre o conteúdo do navegador e o conteúdo do site, como evitar pop-ups de vírus mal-intencionados, reconhecer a importância de sair de sites, os riscos de formulários de preenchimento automático e identificar outros ataques comuns em sites.
- u) Engenharia social – Ministrar e reconhecer táticas comuns de engenharia social, a criar defesas e ter uma perceção sobre como os “engenheiros sociais” pensam.
- v) Informações Pessoais Identificáveis (PII) - Educar colaboradores sobre os diferentes tipos de PII, diretrizes para identificar, recolher e lidar com PII, ações a serem tomadas no caso de uma violação de PII e dicas e técnicas para melhorar a segurança geral de PII.

4.2 As ações de formação referidas no ponto anterior serão realizadas duas vezes ao longo do contrato.

5. Fase 5 – Monitorização e Resposta a incidentes de Segurança

Esta fase visa a gestão do centro de controlo de segurança, (SOC – Security Operations Center), implementado pelo prestador de serviços, oferecendo uma completa visibilidade da segurança das ameaças que afetam a rede de dados dos SMAS DA MAIA, permitindo ao mesmo tempo apoiar na sua mitigação de forma fácil e rápida, quer na Resposta a Incidentes de Segurança ocorridos internamente, externamente (sob os serviços publicados na web) ou alerta de incidentes que ocorreram em outros pontos externos à organização e que possam comprometer os serviços, dados ou aplicações de forma interna.

Nesta fase devem ser garantidas:

- a) Disponibilidade de *call center*, com linha dedicada para incidentes que ocorram na instituição. O centro de controlo de segurança não pode perder vestígios que, de outra forma, seriam tratados como um problema de disponibilidade.
- b) Implementação de contramedidas.
- c) Monitorização em tempo real e análise da triagem / incidente.
- d) Análise de vulnerabilidades e *penetration testing*.
- e) Resposta a incidentes no local;
- f) Mapeamento de rede / *vulnerability scanning*;
- g) Ferramentas de engenharia;
- h) Tuning dos sensores;
- i) Recolher, reter e armazenar dados da auditoria e gestão de conteúdos de auditoria.
- j) Capacidades de resposta a incidentes de segurança
 - i. Descoberta de ativos;
 - ii. Avaliação de vulnerabilidades;
 - iii. Detecção de intrusões;
 - iv. Bloqueio e mitigação de malware/intrusões;
 - v. Monitorização comportamental e heurística;
- k) Funcionalidades e benefícios do centro de controlo de segurança como Serviço
 - i. Recolha de informação passiva
 - ii. Recolha de informação ativa

- iii. Identificação de vulnerabilidades no perímetro de segurança (DMZ), servidores e aplicações Web;
 - iv. Identificação de vulnerabilidades em outros serviços como SNMP/POP3/IMAP, NTP, VPN SSL/IPSEC, DNS, FTP, HTTP/HTTPS, entre outros;
 - v. Exploitation Zero-day/Zero-hour;
 - vi. Injeção de incidentes
 - vii. Land attacks (ataques denial of service)
- l) Descrição de capacidades avançadas
- i. Análise avançada de incidentes e suporte a respostas, como análise digital forense de imagens obtido a partir de memória e disco rígido.
 - ii. Criação e tuning de análises avançadas para detetar modelos de ataque complexos ou avançados, como os utilizados para detetar e seguir os APT's através da nossa ferramenta de MSS do centro de controlo de segurança.
 - iii. Desenvolver ferramentas personalizadas orientadas para detetar, monitorizar, manter (para efeitos de investigação) ou bloquear os APT's em diferentes fases do ciclo de vida dos ciberataques.
 - iv. Exercer e completar uma capacidade de gestão do conhecimento das ameaças, permitindo que os analistas do centro de controlo de segurança interliguem atividades, incidentes, indicadores e diferentes artefactos.
 - v. Acompanhar tendências e elaborar relatórios de atividades e incidentes relacionados com os APT's.
 - vi. Investigação da presença de APT's em redes monitorizadas pelo centro de controlo de segurança.
 - vii. Honeypotting e outros métodos de recolha que permitem à célula coletar, analisar, investigar e monitorizar novas ameaças.
 - viii. Permite o fornecimento de serviços do centro de controlo de segurança mais simples e rápido, através da redução da dependência de terceiros que processam malware e análise forense.

Cláusula 20ª – Prazo de execução

O contrato terá a duração de 12 meses, sendo que cada uma das fases referidas na cláusula anterior terá, aproximadamente, a seguinte duração:

- a) Fase 1 – 1 mês a contar da entrada em vigor do contrato;
- b) Fase 2 – 1 mês a contar da entrada em vigor do contrato;
- c) Fase 3 – 15 dias a contar da entrada em vigor do contrato;
- d) Fase 4 – Nos 2º e 9º mês do contrato.
- e) Fase 5 – Entre o 2º e o último mês de contrato.

Cláusula 22ª – Obrigações dos SMAS da Maia

Compete aos SMAS da Maia nomear o Responsável de Segurança, como sendo o contacto com o prestador de serviços por forma a serem estabelecidos os canais de comunicação necessários, os procedimentos de notificação.