



CONCURSO PÚBLICO N.º 215/20/DCP/ECS/SERVIÇOS DE CIBERSEGURANÇA

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	3
Cláusula 5.ª Condições de pagamento	3
Cláusula 6.ª Propriedade intelectual	4
Cláusula 7.ª Sigilo	4
Cláusula 8.ª Proteção de dados	5
Cláusula 9.ª Cessão da posição contratual e subcontratação	6
Cláusula 10.ª Comunicações e notificações	6
Cláusula 11.ª Penalidades contratuais	7
Cláusula 12.ª Foro competente	7
Cláusula 13.ª Legislação aplicável	7
Cláusulas Técnicas	8
Cláusula 14.ª Descrição técnica do contrato	8
Cláusula 15.ª Afetação de recursos	11
Cláusula 16.ª Perfil técnico dos recursos a afetar aos serviços	12
Cláusula 17.ª Níveis de serviço	12
Cláusula 18.ª Planeamento	13
Cláusula 19.ª Entregáveis e documentação	13
Cláusula 20.ª Gestor do Contrato	14
Cláusula 21.ª Mecanismos formais de acompanhamento	14
ANEXO I	16
ANEXO II	16
ANEXO III	17





CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

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 prestação de serviços continuados de cibersegurança contra intrusão nos sites geridos pela AMA, nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.ª

Local da prestação de serviços

Os serviços são prestados nas instalações do cocontratante.

Cláusula 3.ª

Duração

O contrato terá a duração de 12 meses contados da data da sua celebração, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

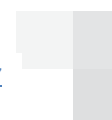
Preço base

1. O preço base é de €62.400 (sessenta e dois mil e quatrocentos euros), a que acresce o IVA À taxa legal em vigor.
2. São excluídas as propostas cujo valor seja superior ao preço base.
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.

Cláusula 5.ª

Condições de pagamento

1. A faturação é efetuada mensalmente mediante a efetiva prestação dos serviços e aceitação pela AMA.
2. O pagamento será efetuado no prazo 30 dias a contar da data da receção das faturas correspondentes, as quais só podem ser emitidas após o vencimento da obrigação a que se referem.
3. As faturas devem discriminar os serviços a que se reportam, o número do contrato bem como o número de





compromisso financeiro associado, o qual será indicado pela AMA, sob pena da sua devolução.

4. Caso as faturas apresentadas não sejam validadas pela AMA esta comunicará tal decisão ao cocontratante para que proceda à sua substituição.
5. As faturas poderão revestir a forma eletrónica, caso em que deverão ser remetidos à AMA através de meio de transmissão escrita e eletrónica de dados para o endereço fornecedores@ama.pt.
6. Só serão devidos os valores referentes às tarefas efetivamente prestadas 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.

Cláusula 6.ª

Propriedade intelectual

São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.

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 ser 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 (UE) 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, pôr 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. Tendo em conta os níveis de serviço estabelecidos na cláusula 17.ª, pelo seu incumprimento poderá ser aplicada uma penalidade de até 1% sobre o valor total do contrato.
2. Pelo incumprimento das obrigações previstas na cláusula 19.ª e 21.ª poderá ser aplicada uma penalidade de até 10% do preço a pagar mensalmente.
3. Em caso de resolução do contrato por incumprimento do cocontratante, a AMA pode exigir-lhe uma pena pecuniária de até 20% do preço contratual.
4. Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo cocontratante ao abrigo do n.º 1, relativamente aos serviços cujo atraso na respetiva conclusão tenha determinado a resolução do contrato.
5. 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.
6. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida nota de crédito.
7. O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.
8. 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 %.
9. 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

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 13.ª

Legislação aplicável

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



CLÁUSULAS TÉCNICAS

Cláusula 14.ª

Descrição técnica do contrato

1. Pretende-se contratar os serviços de uma empresa, que desenvolva para a AMA, num período máximo de 12 meses, um Serviço continuado e persistente de testes de intrusão visando identificar vulnerabilidades na Infraestrutura e camadas aplicacionais da AMA, de forma a detetar e permitir corrigir atempadamente quaisquer eventuais vulnerabilidades de Segurança de Informação que existam.
2. O contratante assegurará à AMA a prestação do Serviço, com o seguinte âmbito:
 - a) Para a realização do Serviço, o esforço total de testes a contratar pela AMA será de 41.000 unidades de serviço por ano.

As unidades de serviço representam o tempo, esforço e complexidade de execução de atividades que compõem os testes de intrusão a realizar, e permitirão que a AMA possa dispor de uma gestão dinâmica da prestação do Serviço.

O proponente deverá incluir na sua proposta a sua tabela de atividades e quantidades de unidades de serviço correspondentes, sendo que a quantidade máxima de unidades de serviço a propor por atividade não deverá exceder as seguintes:

Teste de redes e sistemas (fonte: base OWASP)		
Footprinting	(por endereço IP)	75
Privilege Escalation	(Por Vulnerabilidade)	600
Scanning and Enumeration	(Por Serviço)	75
Vulnerability Analysis	(Por Serviço)	175
Vulnerability Exploitation	(Por Vulnerabilidade)	700
Testes de aplicações Web (fonte: OWASP)		
Authentication Testing	(Por Página)	135
Authorization Testing	(Por Página)	185
Web Services Testing	(Por Parâmetro)	250
AJAX Testing	(Por Parâmetro)	250
Business logic testing	(Por Página)	335
Configuration Management Testing	(Por Página)	100
Data Validation Testing	(Por Parâmetro)	50
Denial of Service Testing	(Por Parâmetro)	135
Information Gathering	(Por Página)	110

Retesting	(Por Teste)	210
Session Management	(Por Aplicação)	550

O proponente deverá incluir na sua proposta a descrição dos testes que se propõe realizar no âmbito da infraestrutura (redes e sistemas) e no âmbito aplicacional;

- b) Testes de intrusão simultâneos a até 15 aplicações web (podem conter ambientes produtivos e não produtivos) e a até 90 IPs ou Hosts, geridos pela AMA.

O contratante deverá assegurar flexibilidade à AMA de modo a que trimestralmente possam ser revistas pela AMA as aplicações e IP's a testar durante os 3 meses seguintes;

- c) Realização, a pedido da AMA, de um conjunto de testes de intrusão simplificados, com o objetivo de o contratante poder disponibilizar resultados preliminares, num prazo mais curto não superior a 2 dias úteis após o respetivo pedido.

Os testes simplificados devem corresponder à realização de testes, com reduzida intervenção manual, focados nas componentes de segurança mais comuns e mais acessíveis para explorar vulnerabilidades;

- d) Testes externos continuados de avaliação da segurança informática (a partir da Internet), sem acesso a quaisquer documentos ou informação sobre a infraestrutura, conforme as categorias referidas nos anexos I a III, não esgotando estas propostas, de modo algum, a multiplicidade de situações que enfrentarão, devendo ser considerada a realidade da AMA em avaliação - tecnologia e serviços, identificando outros testes que se considerem mais adequados;

- e) Repetição de testes após intervenção corretiva da equipa AMA para suprir vulnerabilidades;

- f) Testes iniciais sempre que um novo serviço é publicado e sempre que um atual serviço é alterado, em alinhamento com o processo de gestão da mudança;

- g) Apoio nas instalações da AMA em caso de ciber-ataque, com o objetivo de conter o mesmo e limitar os danos decorrentes.

3. O Proponente deverá assegurar à AMA, os seguintes requisitos para o Serviço a contratar:

- h) Com o objetivo de assegurar a proteção necessária da informação sensível da AMA, os processos de teste a utilizar pelo Proponente devem estar auditados ou credenciados, por auditor ISO27001, no que se refere ao tratamento da informação de Cliente.

- i) O Proponente deve obrigatoriamente apresentar duas cartas de referência de Organismos da Administração Pública relativas à prestação de serviço do mesmo tipo e âmbito requeridos neste caderno de encargos, por pelo menos 2 dois auditores incluídos na equipa por si proposta.

4. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas



cláusulas contratuais, da celebração do contrato decorrerão para o contratante as seguintes obrigações principais:

- a) Prestar os serviços continuados de cibersegurança contra intrusão nos sites geridos pela AMA nos termos previstos nas cláusulas técnicas do presente caderno de encargos;
- b) Analisar e levar em consideração todas as situações e circunstâncias relativas e/ou relevantes para a execução da prestação de serviços, incluindo, entre outras e a título meramente exemplificativo, a informação prévia necessária, as circunstâncias de modo, tempo e lugar e os meios de modo a salvaguardar que os serviços serão prestados nos termos contratados, sem hiatos, falhas ou interrupções que pudessem ter sido previstas;
- c) Assumir todos os riscos inerentes à prestação dos serviços, bem como aqueles que, em concreto, apenas sejam ou possam ser do conhecimento do Prestador de Serviços ou por este gerido em primeira linha;
- d) Garantir, a todo o momento, a correta, completa e adequada articulação e compatibilização entre os serviços prestados e a finalidade a que os mesmos se dirigem com outros serviços ou outras finalidades que com eles estejam ou possam estar em relação, de modo a não afetar negativamente quaisquer outros serviços, produtos ou soluções da AMA, assumindo, em cada momento, o respetivo risco de interface;
- e) Comunicar por escrito à AMA, logo que deles tenha conhecimento, qualquer facto, situação, ocorrência ou vicissitude que torne total ou parcialmente impossível a prestação dos serviços, bem como o cumprimento de qualquer outra das suas obrigações, nos termos do presente caderno de encargos e do Contrato celebrado com a AMA;
- f) Não alterar, por qualquer modo, as condições de prestação dos serviços fora dos casos previstos no presente Caderno de Encargos;
- g) Prestar de forma correta, atempada e fidedigna as informações referentes às condições em que são prestados os serviços, bem como prestar, por escrito ou de forma oral, conforme determinado pela AMA, todos os esclarecimentos que se justifiquem ou que esta entenda necessário;
- h) Executar a prestação dos serviços disponibilizando sempre à AMA aquela que seja, em cada momento e no respeito pelo objeto contratado, a solução mais recente, completa e funcional, obrigando-se a informar imediatamente a AMA caso, durante a prestação de serviços, venham a ocorrer atualizações ou novas funcionalidades inerentes aos serviços contratados, de modo a que a AMA possa, em tempo útil e ao menor custo possível, decidir como livremente entender a esse respeito;
- i) Comunicar por escrito à AMA qualquer facto, situação ou vicissitude que ocorra durante a execução do Contrato a celebrar, e que, relativamente ao cocontratante, altere a sua denominação social, os seus representantes legais, quadros ou funcionários com relevância para a prestação de serviços, a





sua situação jurídica, bem como a sua situação comercial;

- j) Informar, por escrito a AMA, relativamente a qualquer situação por esta indicada referente à execução do Contrato a celebrar, no prazo que lhe vier a ser fixado pela AMA, o qual não poderá ser inferior a 5 (cinco) dias exceto em caso de urgência;
- k) Não afetar os serviços objeto do Contrato a celebrar, a qualquer outra finalidade diferente da prevista no Contrato.
- l) A título acessório, o cocontratante fica ainda obrigado, nomeadamente, a fornecer todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação de serviços, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução dos referidos serviços, nos termos do artigo 452.o do Código dos Contratos Públicos.

Cláusula 15ª

Afetação de recursos

1. Os recursos humanos a afetar à execução dos serviços 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. 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.
6. 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.
7. O cocontratante é responsável pela correta utilização dos bens que, eventualmente, lhe forem confiados, não lhes dando uso diferente do que lhes é devido.
8. No fim do contrato, se aplicável, independentemente do motivo da cessação, o cocontratante obriga-se a devolver os bens que lhe tenham sido confiados, em perfeito estado de utilização.





Cláusula 16.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. Os membros da equipa a afetar aos testes devem demonstrar evidências da sua especialização na prática de testes de segurança da informação, através da publicação individual ou agregada de pelo menos 3 CVEs (Common Vulnerabilities and Exposures) nos últimos 24 meses.
3. O cocontratante deve dispor de uma equipa multidisciplinar de pelo menos 6 Pen-Testers dedicados à função de Testes de Segurança, para apoio e suporte técnico no âmbito deste concurso, com o seguinte perfil:
 - a) O Lead Auditor a suportar a equipa de apoio e suporte técnico no âmbito deste concurso, deve ter uma experiência mínima em TI e Segurança de pelo menos 10 anos de auditoria a segurança de sistemas de informação, e dispor das seguintes certificações:
 - i. OSCP OU GPEN (GIAC);
 - ii. ISO 27001 Lead Auditor;
 - iii. CISSP (ISC2);
 - iv. CISA (ISACA).
 - b) Cada auditor proposto pelo Cocontratante e envolvido no apoio e suporte técnico no âmbito deste concurso deve ter uma experiência mínima em TI e Segurança de pelo menos 3 anos de auditoria a segurança de sistemas de informação, e dispor pelo menos de uma das seguintes certificações mínimas:
 - i. OSCP - Offensive Security Certified Professional;
 - ii. GPEN (GIAC);
 - iii. eWAPTIX - eLearnSecurity Web application Penetration Tester eXtreme.
4. O Gestor de projeto proposto pelo cocontratante e envolvido na prestação dos serviços tem que dispor da certificação profissional PMP, bem como experiência em pelo menos 10 projetos de âmbito similar.

Cláusula 17.ª

Níveis de serviço

1. Os níveis de serviço prestados pelo cocontratante serão avaliados pelos seguintes fatores:
 - a) Reporte de vulnerabilidades: o Cocontratante deve garantir o prazo máximo de 4 horas, após a sua deteção, para o reporte à AMA de qualquer vulnerabilidade crítica.
 - b) Plano de testes: o Cocontratante deve garantir a execução do plano de testes com periodicidade mínima mensal.



- c) Pedido de teste específico da AMA: após um pedido pela AMA para suporte ou enfoque em testes específicos, o cocontratante deve garantir o prazo máximo de 3 dias úteis para finalizar os testes.
 - d) A validação de correções efetuadas pela AMA a vulnerabilidades reportadas deve ser efetuada num prazo máximo de 1 dia útil.
2. O reporte dos Níveis de Serviços será efetuado no máximo mensalmente.

Cláusula 18.ª

Planeamento

A metodologia a utilizar deve contemplar as seguintes fases:

1. Auditoria inicial de segurança:

Os serviços deverão iniciar-se obrigatoriamente até uma semana após celebração do contrato.

Esta atividade deve ocorrer durante o mês 1 de vigência do contrato, englobando as seguintes atividades:

- a) Execução de testes a todas as aplicações *web* indicados pela AMA, conforme descrito na cláusula 14ª;
- b) Instalação da ferramenta colaborativa em infraestrutura a fornecer pela AMA;
- c) Disponibilização do resultado dos testes na ferramenta colaborativa.

2. Serviço continuado de cibersegurança:

Esta atividade ocorre continuamente entre o mês 2 e o mês 12, englobando as seguintes atividades:

- a) Testes mensais automatizados de vulnerabilidades a todas as aplicações *web* constantes do inventário da ferramenta colaborativa;
- b) Execução de uma média de cinco testes mensais específicos de penetração;
- c) Execução mensal de testes específicos de vulnerabilidades a uma lista de até cinco aplicações a fornecer;
- d) Execução de testes conforme descrito na cláusula 14ª;
- e) Atualização permanente dos dados registados na ferramenta colaborativa.

3. Apoio em caso ciber-ataque:

Este serviço está ativo do mês 1 ao mês 12 e tem o perfil descrito na cláusula 14ª.

Cláusula 19.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*) a instalar pelo fornecedor na infraestrutura da AMA, que assegure os mecanismos de proteção e segurança da informação sobre as vulnerabilidades e da informação de todas as comunicações entre o cocontratante e AMA.
- 2. O cocontratante deverá obrigatoriamente disponibilizar a seguinte informação na plataforma colaborativa:



- a) Vulnerabilidades: contendo entidade, descrição resumida, sistemas afetados, data deteção, recomendação, prioridade, custo de implementação se aplicável;
- b) Comunicação de vulnerabilidades: comunicação trocada com a AMA;
- c) Quadro resumo: identificando quais os sistemas, serviços, aplicações e funcionalidades testadas, status do teste, resultado do teste e identificação das evidências associadas;
- d) Relatório dinâmico de serviços, com pelo menos a seguinte informação:
 - i. Âmbito (Enumerando os sistemas, redes, etc, analisados);
 - ii. Conclusões;
 - iii. Análise detalhada contemplando:
Descrição das vulnerabilidades, incluindo “proof of concept”, grau de criticidade e risco, bem como consequências práticas em termos de risco de negócio, acompanhada de recomendações para correção;
 - iv. Recomendações.

Cláusula 20.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.

Cláusula 21.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.





ANEXO I

Testes às Vulnerabilidades na Infraestrutura

Categoria	Objetivos
Levantamento da Rede / Enumeração da Rede	Descobrir dispositivos Identificar paths das comunicações e facilitar determinação da arquitetura de rede
Portas de Rede e Identificação de Serviços	Descobrir dispositivos Ativos Descobrir portas abertas e serviços/aplicações associadas
Análise/Scanning de Vulnerabilidades	Identificar IPs e portos abertos Identificar vulnerabilidades conhecidas Identificar vulnerabilidades desconhecidas Facultar assessoria na mitigação das vulnerabilidades descobertas
Password Cracking	Identificar passwords e políticas de passwords não robustas

ANEXO II

Testes às Vulnerabilidades nas Aplicações Web

Categoria	Objetivos
Recolha e compilação da informação	Recolher o máximo de informação possível sobre uma aplicação-alvo
Testes às Configurações de Gestão	Analisar a infraestrutura e topologia da arquitetura
Testes às Autenticações	Perceber como funciona o processo de autenticação e usar a informação para subverter o mecanismo de autenticação
Gestão das Sessões	Segurança da Aplicações
Testes às Autorizações	Possibilidade de ultrapassar o esquema de autorizações Encontrar maneiras para escalar privilégios
Testes à lógica do negócio	Vulnerabilidades relacionadas com o negócio
Testes à Validação de Dados	Aplicação valida de forma suficiente dados de entrada antes de os utilizar
Testes aos Serviços Web	Vulnerabilidades nos Serviços Web
Testes AJAX	Vulnerabilidades Asynchronous JavaScript and X





ANEXO III

Testes aplicacionais exaustivos

No mínimo, deverão ser executados os Testes abaixo identificados em função dos tipos de ativos objeto de teste:

- XSS Persistente;
- XSS Refletido;
- Execução de código aplicacional arbitrário remotamente;
- Execução de comandos SQL arbitrários através da aplicação (SQL Injection);
- Execução de pedidos SOAP arbitrários a partir da aplicação (SOAP Injection);
- Execução de queries LDAP arbitrárias através da aplicação (LDAP Injection);
- Path arbitrárias através da aplicação (Ex: PATH Injection);
- Manipulação de valores em Hidden Fields;
- Manipulação de valores em Cookies e headers;
- Manipulação de parâmetros submetidos;
- Bypass de validações de segurança realizadas unicamente do lado do cliente (ex:JavaScript);
- Alteração do fluxo aplicacional em processos multi-etapa;
- Utilização incorrecta de estados/relações de confiança na aplicação;
- Realização de transacções não previstas.

