



**CONCURSO PÚBLICO N.º 51/22/DCP/EGSIPD/SUBSCRIÇÃO DE
PLATAFORMA TECNOLÓGICA DE SUPORTE À GESTÃO DE
CONFORMIDADE E SERVIÇOS DE CONSULTORIA DE SEGURANÇA DE
INFORMAÇÃO E DADOS PESSOAIS**

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	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 Foro competente	8
Cláusula 13.ª Legislação aplicável	8
Cláusulas Técnicas	9
Enquadramento	9
Cláusula 14.ª Descrição técnica do contrato	9
Cláusula 15.ª Requisitos específicos para o tratamento de dados pessoais	13
Cláusula 16.ª Requisitos específicos de implementação para a segurança da informação	13
Cláusula 17.ª Perfil técnico dos recursos a afetar aos serviços	13
Cláusula 18.ª Substituição das equipas	14
Cláusula 19.ª Níveis de serviço	15
Cláusula 20.ª Formação	15
Cláusula 21.ª Entregáveis e documentação	16
Cláusula 22.ª Gestor do Contrato	16
Cláusula 23.ª Mecanismos formais de acompanhamento	16
Cláusula 24.ª Acesso a informação da AMA	16

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 aquisição de subscrição de plataforma tecnológica para a gestão de conformidade de referenciais normativos e de serviços de consultoria de Segurança da Informação e Dados Pessoais, nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.ª

Local da prestação de serviços

Os serviços de consultoria serão prestados nas instalações do cocontratante e a subscrição da Plataforma será disponibilizada em modelo SaaS.

Cláusula 3.ª

Duração

O contrato inicia-se na data da sua celebração e cessa em 31/12/2023, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preço base

1. O preço base é de € 206.961,00(duzentos e seis mil novecentos e sessenta e um euros), a que acresce o IVA à taxa legal em vigor, distribuindo-se da seguinte forma:
 - a) Subscrição da Plataforma de Gestão de conformidade, migração para nova plataforma, configuração de todo o Sistema de Gestão de Segurança de Informação e Gestão Dados Pessoais com o preço base de € 93 375,00;
 - b) Serviços de consultoria de apoio na gestão e operação da Plataforma, de segurança da informação e de proteção de dados pessoais com o preço base de € 113 586,00;
2. São excluídas as propostas que apresentem qualquer preço superior aos preços indicados no número 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.

Cláusula 5.ª

Condições de pagamento

1. A faturação é efetuada nos seguintes termos:
 - a) Para a subscrição da Plataforma a faturação será realizada anualmente;
 - b) Para os serviços de consultoria, referentes à alínea b) do n.º 1 da Cláusula 4ª, a faturação é emitida com periodicidade mensal, de acordo com os serviços efetivamente prestados no mês anterior, e após validação pela AMA do respetivo relatório mensal de horas consumidas no mês que antecede
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 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 ou, caso não seja possível, 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

1. São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
2. O cocontratante obriga-se a transferir a posse e a propriedade dos elementos a desenvolver ao abrigo do contrato para a AMA incluindo os direitos autorais sobre todas as criações intelectuais abrangidas pelos serviços a prestar, incluindo os previstos no n.º 4 do artigo 14.º e 49.º, ambos do Código do Direito de Autor e dos Direitos Conexos, bem como de outros direitos de propriedade intelectual, relativos aos serviços objeto do presente caderno de encargos, produtos dele resultantes nomeadamente, código fonte,





documentação e elementos afins, bem como dos produtos consequentes a todas as ulteriores adaptações que se venham a revelar necessárias.

3. O cocontratante entregará à AMA no termo do contrato toda a documentação e desenvolvimento, relativo aos trabalhos desenvolvidos, incluindo as respetivas fontes que serão propriedade da AMA.
4. A AMA poderá transformar e reproduzir todos os documentos e todo o software desenvolvido, bem como proceder à sua distribuição, onerosa ou gratuita, de forma inteiramente livre.
5. Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente caderno de encargos.

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 (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. Pelo incumprimento de obrigações emergentes do contrato, a AMA pode exigir ao cocontratante o pagamento de uma sanção pecuniária, num montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
 - a) Pelo incumprimento na disponibilização do acesso à Plataforma num prazo inferior a 5 dias úteis após a data de início do contrato, será aplicada uma penalidade equivalente a 0,25% do valor de aquisição por cada dia em atraso;
 - b) Pelo incumprimento do prazo de migração da Plataforma no prazo indicado no n.º 2 da Cláusula





- 19ª, será aplicada uma penalidade equivalente a 0,25% do valor de aquisição por cada dia em atraso;
- c) Pela indisponibilidade de recursos com o perfil adequado à prestação de serviços de acordo com o especificado no presente Caderno de Encargos, será aplicada uma penalidade equivalente a 0,25% do valor dos serviços por cada dia de indisponibilidade;
 - d) Pela indisponibilidade no âmbito da plataforma objeto do contrato será aplicada uma penalidade equivalente a 1% do valor de aquisição por dia de indisponibilidade;
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 nota de crédito.
 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

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

Enquadramento

A AMA adquiriu no final de 2018 a subscrição da plataforma de gestão da conformidade Integrity GRC que disponibiliza diversos mecanismos que permitem a gestão da conformidade pelo suporte à execução de inquéritos de forma integrada com os restantes processos de planeamento, implementação, avaliação e melhoria. Neste ciclo inserem-se funcionalidades de cadastro de ativos, identificação e gestão de vulnerabilidades e ameaças, a avaliação e mitigação de risco, a identificação e atribuição de tarefas suportadas por *workflows*, avaliação do grau de execução e *reporting*, bem como a associação das atividades e artefactos aos requisitos dos referenciais normativos, atestando a conformidade. Pretende-se com o presente procedimento uma nova subscrição da plataforma de gestão da conformidade Integrity GRC, do tipo ou equivalente, garantindo desta forma a continuidade do trabalho já desenvolvido. Caso seja uma Plataforma equivalente é necessário ser assegurada a migração e configuração da nova Plataforma e asseguradas todas as funcionalidades, atividades e *workflows* já definidos na Plataforma atual.

Cláusula 14.ª

Descrição técnica do contrato

1. O presente procedimento tem por objetivo:

- a) A subscrição da plataforma de suporte à gestão de conformidade para um número mínimo de 100 utilizadores e 6 árvores de conformidade com referenciais normativos e legais, nomeadamente ISO, Decreto-Lei n.º 65/2021, Quadro Nacional de Referência para a Cibersegurança (QNRCS), Lei n.º 58/2019, Regulamentos e/ou Diretivas da Comissão Europeia e normas conexas;
- b) A aquisição de serviços de consultoria para configuração de novos referenciais normativos, apoio na expansão da certificação ISO 27001 a novos sistemas da AMA e sua configuração na Plataforma, apoio na conformidade dos sistemas da AMA com o QNRCS e sua configuração na Plataforma como árvore de conformidade, apoio na conformidade dos sistemas da AMA com o Decreto-Lei n.º 65/2021, alterações aos registos de tratamento na Plataforma, elaboração de questionários de DPIA na Plataforma, definição de *workflow* de gestão de pedidos dos titulares de dados e de gestão de incidentes na Plataforma, formação sobre DPIA, incidentes e guia de utilização e auditorias a efetuar no âmbito da conformidade com o RGPD.

2. A plataforma de suporte à gestão de conformidade deverá suportar as seguintes funcionalidades base:

- a) Gestão de utilizadores
 - i. Gestão de permissões de utilizadores e grupos, segregadas por árvores de conformidade, documentos (políticas e procedimentos, evidências), *Dataforms*



- (instâncias e Identificador de registo dentro do *dataform*), ativos, riscos e controlos/medidas, atividades de *workflows*;
 - ii. Gestão de grupos e atribuição de utilizadores a grupos;
 - iii. Mecanismos de autenticação segura, sendo valorizada a utilização da plataforma de autenticação transversal à Administração Pública “Autenticação.gov” ou autenticação com duplo fator;
 - iv. *Workflows* para controlo de execução de processos/atividades, validação e aprovação de/a utilizadores/grupos;
 - v. Funcionalidades de suporte à utilização concorrente de documentos;
 - vi. Registo das atividades dos utilizadores sobre documentos;
- b) Gestão de referenciais de conformidade:
- i. Criação e configuração de árvores de conformidade;
 - ii. Avaliação da resposta aos questionários de diferentes áreas organizacionais e/ou fornecedores/parceiros;
 - iii. Gestão Documental para Políticas, Processos, Procedimentos e Registos associados aos referenciais de conformidade, permitindo a definição do seu ciclo de vida, definição e atribuição de classificação, definição e atribuição de responsabilidades a utilizadores/grupos, estados, referenciação em mais do que um sistema de conformidade, gestão de versões, atribuição de metadados;
 - iv. Gestão de Atividades (calendarização e atribuição a utilizadores/grupos);
 - v. Possibilidade de associar as atividades aos documentos e requisitos nas árvores de conformidade;
 - vi. Possibilidade de atribuição de atividades e responsabilidades aos diferentes utilizadores com registo das mesmas para suporte à rastreabilidade das atividades (*logging*);
 - vii. Funcionalidades de *workflow* associado às árvores de conformidade, que permitam a criação e configuração, bem como a atribuição de atividades e responsabilidades (utilizadores/grupos);
 - viii. Definição de métricas de evolução e cumprimento de atividades;
 - ix. Avaliação da conformidade e da sua maturidade para cada uma das árvores configuradas;
 - x. Disponibilização das árvores de conformidade de forma integrada com os recursos do sistema;
- c) Suporte à Implementação da conformidade
- i. Gestão de risco



1. Gestão do ciclo de vida do risco por âmbito e usando em paralelo metodologias diferentes para identificação do risco
 2. Definição de grau/escala de classificação do risco
 3. Configuração de tipologias de risco
 4. Definição de componentes e algoritmo de avaliação
 5. Definição e associação de atividades de tratamento
 6. Definição, configuração de *workflows* de controlo de atividades e responsabilidades (utilizadores/grupos)
 7. Definição e configuração de critérios de aceitação
 8. Definição de indicadores de avaliação
 9. Associação de riscos e controlos/medidas a utilizadores/grupos de utilizadores
- ii. Gestão de ativos
1. Cadastro pelo recurso a formulários ou importação em formato aberto
 2. Associação de ameaças, vulnerabilidades e relação com a gestão de risco
 3. Associação de riscos, medidas, utilizadores/grupos e requisitos de conformidade
- d) Recolha de informação, análise e relatórios
- i. Criação, configuração e gestão de formulários/questionários;
 - ii. Criação, configuração e gestão de *ckecklist* de auditoria associadas às árvores de conformidade configuradas;
 - iii. Criação e configuração de mapas de monitorização do estado das atividades atribuídas a utilizadores/grupos e de *logging*;
 - iv. Configuração de mapas de monitorização de métricas com métricas configuráveis de acordo com os parâmetros de cada uma das atividades;
 - v. Criação de mapas de acompanhamento do nível de conformidade e estágios de maturidade ao longo do tempo para as várias áreas organizacionais e/ou parceiros;
 - vi. Identificação e gestão de ameaças e vulnerabilidades e criação de mapas em contexto de ativos, análise de risco e atividades de mitigação
 - vii. Análise de resultados e indicadores de risco e/ou de conformidade
 - viii. Relatórios de *logging*, pedidos de alteração e não-conformidades;
 - ix. Elaboração automática de relatórios que relacionem registos e grau de conformidade relativamente as várias árvores de conformidade configuradas
 - x. Possibilitar a atribuição de itens de Tratamento de Risco aos utilizadores, por forma a garantir a sua efetiva gestão e *tracking*;
 - xi. Possibilidade de realização de múltiplas ações de análise de risco em simultâneo;





- xii. Suportar a configuração de critérios de aceitação de risco como suporte ao processo de Gestão de Risco;
 - xiii. Disponibilização de notificações internas e por *e-mail*, para cada utilizador/grupo que lhes permita gerir as suas interações com o sistema, responsabilidades e restantes recursos;
 - xiv. Capacidade de exportação das diferentes árvores de conformidades para documento de suporte a auditorias relativamente às árvores de conformidade configuradas;
 - xv. Dispor de módulo de pesquisa global e ampla que permita a realização de ações de pesquisa sob os mais diversos recursos da plataforma
 - xvi. Configuração de relatórios e mapas (layout, títulos, *headers* e *footers*, fonte, idioma)
 - xvii. Os relatórios, mapas e *checklist* deverão ser exportados em formatos abertos editáveis
- e) Gestão de informação e atributos de referência
- i. Criação, edição e eliminação de atributos específicos garantindo a integridade referencial na edição e eliminação;
 - ii. Criação, edição e eliminação de listas de opções específicas garantindo a integridade referencial na edição e eliminação.
3. A consultoria é prestada tendo em consideração uma bolsa de 1721 horas onde serão prestados, entre outros, os seguintes serviços:
- a) configurações da plataforma a efetuar no início da subscrição para adaptação às novas árvores de conformidade, nomeadamente a do QNRCS;
 - b) apoio na expansão da certificação ISO 27001 a novos sistemas da AMA (pelo menos 3 novos sistemas em 2022 e 5 novos sistemas em 2023) e sua integração e configuração na Plataforma;
 - c) apoio na conformidade dos sistemas da AMA com o QNRCS e sua integração e configuração na Plataforma;
 - d) apoio na conformidade dos sistemas da AMA com o Decreto-Lei n.º 65/2021 e sua integração e configuração na Plataforma;
 - e) apoio no processo de gestão de risco referente à norma ISO 27001;
 - f) apoio nas alterações aos registos de tratamento na Plataforma;
 - g) elaboração de questionários de DPIA na Plataforma;
 - h) definição de *workflow* de gestão de pedidos dos titulares de dados e de gestão de incidentes na Plataforma;
 - i) realização de auditorias internas a efetuar no âmbito da conformidade com o RGPD e RCM41/2018;
 - j) realização de formação sobre DPIA, incidentes e guia de utilização;
 - k) Carregamento e validação do risco dos tratamentos de dados pessoais na Plataforma.
4. No final do contrato, se solicitado pela AMA, o cocontratante deverá assegurar a exportação estruturada





de dados, processos, documentos, em formatos abertos, de acordo com a RCM nº 2/2018, de toda a informação depositada e processada ao abrigo da subscrição adquirida no âmbito do presente caderno de encargos, após o que assegurará a eliminação de toda a informação relativa à AMA.

Cláusula 15.ª

Requisitos específicos para o tratamento de dados pessoais

Para dar cumprimento às normas do Regulamento Geral de Proteção de Dados em matéria de arquitetura de segurança das redes e sistemas de informação, o cocontratante deve garantir, quando aplicáveis no âmbito do presente caderno de encargos, todos os requisitos específicos constantes da RCM n.º 41/2018 classificados como obrigatórios.

Cláusula 16.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. 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*.
3. 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.
4. O fornecedor fica sujeito a política de Gestão de Fornecedores.
5. 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.

Cláusula 17.ª

Perfil técnico dos recursos a afetar aos serviços

1. O cocontratante deverá disponibilizar, no mínimo, um recurso para cada um dos 3 perfis a seguir indicados, os quais devem compreender os seguintes requisitos mínimos para execução do contrato:
 - a) Perfil 1:
 - Formação académica (ex. licenciatura, pós-graduação, mestrado) numa das seguintes áreas de Segurança de Informação, Sistemas e Tecnologia de Informação, Cibersegurança e Proteção de Dados Pessoais;
 - Experiência superior a 9 anos área da gestão operacional de infraestruturas TIC;
 - Conhecimento de configuração de processos, *workflows*, atividades e implementação de árvores de conformidade na plataforma de gestão de conformidade no âmbito do





presente caderno de encargos;

- Experiência comprovada superior a 3 anos na implementação de sistemas de gestão de segurança de informação de acordo com a norma ISO/IEC 27001-2013;
- Lead Auditor certificado em ISO 27001;
- Lead Implementer certificado em ISO 27001;
- Certificação COBIT 5

b) Perfil 2:

- Formação académica (ex. licenciatura, pós-graduação, mestrado) numa das seguintes áreas de Segurança de Informação, Sistemas e Tecnologia de Informação, Cibersegurança e Proteção de Dados Pessoais;
- Conhecimento de configuração de processos, *workflows*, atividades e implementação de árvores de conformidade na plataforma de gestão de conformidade no âmbito do presente caderno de encargos;
- Experiência comprovada superior a 3 anos na implementação de sistemas de gestão de proteção de dados pessoais
- Lead Auditor certificado em ISO 27001;
- Certificação CISM;
- Certificação CRISC.

c) Perfil 3:

- Formação académica superior em Engenharia Informática;
- Experiência superior a 10 anos área da gestão operacional de TIC com destaque para projetos de segurança da informação e gestão do risco;
- Conhecimento de configuração de processos, *workflows*, atividades e implementação de árvores de conformidade na plataforma de gestão de conformidade no âmbito do presente caderno de encargos;
- Lead Auditor certificado em ISO 27001;
- Certificação CISM;
- Certificação CISA;
- Certificação CRISC.

Cláusula 18.^a

Afetação de recursos e a sua substituição das equipas

1. Qualquer alteração à composição da equipa indicada em sede de formação do contrato deve ser previamente comunicada à AMA e só será aceite caso reúna os requisitos mínimos exigidos na cláusula





anterior, podendo, para o efeito, ser solicitada informação e documentação adicional para confirmação dos elementos curriculares apresentados.

2. A substituição referida no número anterior deverá ocorrer da seguinte forma:
 - a) O cocontratante deverá, em 5 dias úteis, identificar o seu melhor recurso considerando os requisitos mínimos exigidos e obter a aceitação pela AMA;
 - b) O cocontratante deverá assegurar que nos 5 dias úteis após a aceitação o recurso inicia a prestação do serviço.
3. 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 comumente expectável, poderá a AMA exigir a sua substituição, aplicando-se, com as devidas adaptações, o disposto nos números anteriores.

Cláusula 19.ª

Níveis de serviço

1. O acesso à Plataforma deverá estar disponível a partir da data de assinatura do contrato;
2. Caso exista necessidade de migração da Plataforma, os sistemas deverão estar totalmente operacionais (inclui configuração das 5 árvores de conformidade atualmente existentes, com toda a documentação e associação desta documentação aos requisitos das normas ISO 27001, Proteção de Dados Pessoais e ETSI EN 319 401, registo dos ativos de segurança da informação e proteção de dados, 4 levantamentos e tratamento de riscos, 4 *workflows*, registo das atividades e formulários atualmente existentes) no prazo de 20 dias úteis a partir da data de celebração do contrato
3. A plataforma no âmbito do contrato deverá apresentar uma disponibilidade mínima de 99,5%.
4. Deverão ser assegurados serviços de suporte a eventuais incidentes de segurança com um tempo de resposta inferior a 12h;
5. Devera ser assegurada a disponibilidade da equipa com o perfil requerido para consultoria com marcação prévia de 24h para uma sessão mínima de 4h de trabalho.

Cláusula 20.ª

Formação

1. O cocontratante obriga-se a ministrar uma sessão de formação, com uma duração mínima de 32 horas, no caso de migração para nova Plataforma sobre todas as funcionalidades da Plataforma, não podendo exigir qualquer quantia adicional relacionada com a formação.
2. O cocontratante obriga-se a ministrar duas sessões de formação aos colaboradores da AMA relativamente às áreas de segurança da informação e dados pessoais, fazendo parte da bolsa de horas de consultoria;
3. As formações decorrerão nas instalações da AMA, em prazo a acordar entre as partes, devendo ser previamente aprovadas pelo gestor de projeto.





Cláusula 21.ª

Entregáveis e documentação

1. O cocontratante deverá entregar:
 - a) Manuais de utilização;
 - b) Relatórios dos serviços de consultoria prestados;
 - c) Relatórios de acompanhamento de pedidos de suporte.

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

Mecanismos formais de acompanhamento

1. O cocontratante deverá fornecer à AMA um relatório sobre os trabalhos realizados no âmbito dos serviços de consultoria
2. O cocontratante deverá fornecer mensalmente relatório escrito do suporte solicitado pela AMA na utilização da plataforma;
3. O cocontratante deverá informar a AMA de imediato sobre incidentes de segurança de que a plataforma seja alvo com impacto direto ou indireto sobre integridade, disponibilidade e confidencialidade dos dados suportados e/ou na funcionalidade da plataforma no âmbito da licença subscrita e fornecer em relatório mensal a descrição detalhada, impacto sobre a informação no âmbito e medidas corretivas aplicadas;
4. Em caso de indisponibilidade da Plataforma o cocontratante deverá entregar toda a informação nela contida requerida pela AMA no prazo máximo de 3 horas.

Cláusula 24.ª

Acesso a informação da AMA

No decorrer do contrato o cocontratante poderá ter acesso a informação classificada com os níveis restrito e





confidencial. Terá ainda acesso a toda a informação recolhida no decorrer dos serviços de consultoria prestados, devendo desta forma ter especial cuidado no cumprimento da Cláusula 7ª.

