



REGIÃO AUTÓNOMA DOS AÇORES
Presidência do Governo Regional
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

CADERNO DE ENCARGOS

**Consultoria técnica para o desenvolvimento e consolidação de
manuais de boas práticas de utilização de meios informáticos e de
cibersegurança**



REGIÃO AUTÓNOMA DOS AÇORES
Presidência do Governo Regional
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

ÍNDICE

CLÁUSULAS JURÍDICO-ADMINISTRATIVAS	3
Cláusula 1. ^a Objeto	3
Cláusula 2. ^a Local da prestação de serviços	3
Cláusula 3. ^a Preço base	3
Cláusula 4. ^a Duração do contrato	3
Cláusula 5. ^a Condições de pagamento	3
Cláusula 6. ^a Direitos de propriedade intelectual e industrial	4
Cláusula 7. ^a Sigilo	4
Cláusula 8. ^a Proteção de dados pessoais	5
Cláusula 9. ^a Cessão da posição contratual e subcontratação	5
Cláusula 10. ^a Casos Fortuitos ou de Força Maior	5
Cláusula 11. ^a Deveres de colaboração recíproca e informação	6
Cláusula 12. ^a Seguros	6
Cláusula 13. ^a Foro competente	7
Cláusula 14. ^a Legislação aplicável	7
CLÁUSULAS TÉCNICAS	7
Cláusula 15. ^a Descrição técnica do contrato	7
Cláusula 16. ^a Mecanismos formais de acompanhamento	7
Cláusula 17. ^a Sanções.....	8
ANEXO I	9



CLÁUSULAS JURÍDICO-ADMINISTRATIVAS

Cláusula 1.^a

Objeto

O contrato a celebrar tem como objeto a aquisição de serviços de “Consultoria técnica para o desenvolvimento e consolidação de manuais de boas práticas de utilização de meios informáticos e de cibersegurança”, nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.^a

Local da prestação de serviços

1. Os serviços são prestados remotamente e/ou presencialmente, nas instalações da Direção Regional das Comunicações, sita na Rua Dr. José Bruno Tavares Carreiro, n.º 6 - 8º Piso, 9500-119 Ponta Delgada, ilha de São Miguel, conforme definido nas cláusulas técnicas.
2. Todas as despesas relativas a deslocações e alojamento estão incluídas no preço constante da proposta.

Cláusula 3.^a

Preço base

1. O preço base é de 55.000,00€ (cinquenta e dois mil e duzentos euros).
2. São excluídas as propostas cujo valor seja superior ao preço base.

Cláusula 4.^a

Duração do contrato

O contrato terá a duração de 30 dias contados da data na assinatura do contrato, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 5.^a

Condições de pagamento

1. A faturação é efetuada nos seguintes termos:
 - a) 40% com entrega e aceitação do Manual de governança, de exploração de sistemas de informação e de cibersegurança da Administração Pública Regional, conforme previsto no Anexo I ao Caderno de Encargos;
 - b) 30% com a entrega e aceitação do Manual do utilizador da Administração Pública Regional de meios informáticos e de cibersegurança, conforme previsto no Anexo I ao Caderno de Encargos;
 - c) 15% com a entrega e aceitação do Manual de boas práticas de cibersegurança para PMEs, conforme previsto no Anexo I ao Caderno de Encargos;
 - d) 15% com a entrega e aceitação do Manual de boas práticas de cibersegurança para freguesias e municípios, conforme previsto no Anexo I ao Caderno de Encargos.



REGIÃO AUTÓNOMA DOS AÇORES
Presidência do Governo Regional
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

2. O pagamento será efetuado no prazo máximo de 60 (sessenta) 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. Nos termos da Lei n.º 8/2012, de 21 de fevereiro, a entidade adjudicante emite um número de compromisso válido e sequencial, que o cocontratante deverá indicar nas faturas.
4. Desde que devidamente emitidas e observado o disposto na presente cláusula, as faturas são pagas através de transferência bancária, para o NIB a indicar pelo cocontratante.
5. O cocontratante não pode efetuar a transmissão de créditos ao abrigo de contratos de factoring ou proceder à cessão de créditos, sem autorização prévia da entidade adjudicante.

Cláusula 6.ª

Direitos de propriedade intelectual e industrial

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 entidade adjudicante incluindo os direitos autorais sobre todas as criações intelectuais abrangidas pelos serviços a prestar, bem como de outros direitos de propriedade intelectual, relativos aos serviços objeto do presente caderno de encargos, produtos dele resultantes nomeadamente, 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 entidade adjudicante no termo do contrato toda a documentação e desenvolvimento, relativo aos trabalhos desenvolvidos, incluindo as respetivas fontes que serão propriedade da entidade adjudicante.
4. A entidade adjudicante poderá transformar e reproduzir todos os documentos desenvolvidos, 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 entidade adjudicante 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.



REGIÃO AUTÓNOMA DOS AÇORES
Presidência do Governo Regional
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

4. O cocontratante assume igualmente o compromisso de remover e destruir, no final do contrato, todo e qualquer registo, eletrónico ou em papel, relacionado com os dados e processos analisados e que a entidade adjudicante 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 entidade adjudicante, nos termos legalmente previstos na Lei n.º 58/2019, de 8 de agosto.
6. 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 pessoais

1. O cocontratante garante o cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, designadamente o disposto no artigo 28.º, bem como legislação complementar aplicável.
2. Quando solicitado, o cocontratante obriga-se a apresentar ao contraente público, no prazo de 48 horas, as medidas adotadas que evidenciam o cumprimento as disposições relativas à proteção de dados pessoais.

Cláusula 9.ª

Cessão da posição contratual e subcontratação

O cocontratante não pode ceder a sua posição no contrato ou subcontratar total ou parcialmente os serviços incluídos no mesmo sem autorização prévia da entidade adjudicante.

Cláusula 10.ª

Casos Fortuitos ou de Força Maior

1. Não podem ser impostas penalidades ao cocontratante, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;



REGIÃO AUTÓNOMA DOS AÇORES
Presidência do Governo Regional
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte, bem como informar o prazo previsível para restabelecer a situação.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 11.^a

Deveres de colaboração recíproca e informação

As partes estão vinculadas pelo dever de colaboração mútua, designadamente no tocante à prestação recíproca de informações necessárias á boa execução do contrato, sem prejuízo dos deveres de informação previstos no artigo 290.º do CCP.

Cláusula 12.^a

Seguros

1. É da responsabilidade do cocontratante a cobertura, através de contratos de seguro de responsabilidade civil extracontratual destinados a garantir o ressarcimento dos danos causados a terceiros por atos ou omissões negligentes, nos termos da legislação em vigor, e de riscos de acidentes de trabalho e doenças profissionais, devendo nas apólices constar uma cláusula pela qual a entidade se compromete a mantê-las válidas até à conclusão da prestação de serviços.
2. O contraente público pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos no número anterior, à exceção dos que foram exigidos nos documentos de habilitação, devendo o cocontratante fornecê-la no prazo 5 (cinco) dias.



REGIÃO AUTÓNOMA DOS AÇORES
Presidência do Governo Regional
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

3. As condições estabelecidas nos números anteriores abrangem igualmente a atividade dos empregados, assalariados, mandatários ou pessoas diretamente envolvidas na atividade do segurado quando ao serviço deste e desde que sobre elas recaia também a obrigação de indemnização, bem como os eventuais consultores que venham a ser agregados, mesmo que em tempo restrito, respondendo o prestador de serviço perante a contraente público pela sua observância.
4. Os encargos referentes aos seguros impostos por este Caderno de Encargos, bem como qualquer dedução efetuada pela seguradora a título de franquia em caso de sinistro indemnizável, correm por conta do prestador de serviços.

Cláusula 13.^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 Ponta Delgada.

Cláusula 14.^a

Legislação aplicável

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

CLÁUSULAS TÉCNICAS

Cláusula 15.^a

Descrição técnica do contrato

O objeto do contrato consiste na prestação de serviços de consultoria técnica para o desenvolvimento e consolidação de manuais de boas práticas de utilização de meios informáticos e de cibersegurança, de acordo com as características, especificações e quantidades que constam do Anexo I ao presente caderno de encargos.

Cláusula 16.^a

Mecanismos formais de acompanhamento

1. Os entregáveis previstos no Anexo I estão sujeitos a aceitação expressa da entidade adjudicante.
2. Se o previsto na alínea anterior, não estiver de acordo com o pretendido pela entidade adjudicante, o adjudicatário deverá proceder à sua alteração, em conformidade com as exigências do caderno de encargos, devendo esta definir o prazo máximo, em dias para a sua alteração/modificação, na comunicação formal de não aceitação.



REGIÃO AUTÓNOMA DOS AÇORES

Presidência do Governo Regional

DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

3. Deve o adjudicatário estar disponível para sessões/reuniões presenciais e remotas, sempre que a entidade adjudicante entenda necessário.
4. Deve o adjudicatário cumprir a seguinte calendarização dos trabalhos:
 - a. 1ª semana: sessão de arranque dos trabalhos e levantamento/mapeamento, em articulação com as equipas técnicas da DRCTD, das especificidades e medidas técnicas e organizativas conducentes à elaboração do Manual de governança, exploração de sistemas de informação e de cibersegurança da Administração Pública Regional e do Manual do utilizador da Administração Pública Regional de meios informáticos e de cibersegurança;
 - b. 2ª, 3ª e 4ª semanas: reuniões remotas para ponto de situação dos trabalhos desenvolvidos e validação dos documentos em produção ou já produzidos.

Cláusula 17.ª

Sanções

1. Pelo incumprimento de obrigações emergentes do contrato, a entidade adjudicante 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 dos prazos de entrega até 1% do preço contratual, por cada dia de atraso;
2. Na determinação da gravidade do incumprimento, a entidade adjudicante 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 entidade adjudicante decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.



ANEXO I

1. Caracterização geral dos serviços

A cibersegurança e ciberdefesa posicionam-se atualmente como fatores determinantes para a garantia do sucesso e da resiliência das sociedades, assim como das organizações e dos indivíduos que as integram. Com o desenvolvimento ubíquo das iniciativas e soluções que tornam a nossa vivência cada vez mais digital, importa estabelecer estratégias e mobilizar recursos capazes de dar resposta adequada às ameaças e aos riscos crescentes.

O Regulamento Cibersegurança da União Europeia define a cibersegurança como "as atividades necessárias para proteger a rede e os sistemas de informação, os utilizadores desses sistemas e outras pessoas afetadas pelas ciberameaças". No relatório do The Global Risks Report 2021 do Fórum Económico Mundial, no top 10 de riscos por probabilidade de ocorrência, as falhas de cibersegurança ocupam a 9ª posição, demonstrando a preocupação crescente com este tipo de ameaças.

Atendendo ao número crescente de ciberataques de forma transversal em todos os setores, públicos ou privados, importa estabelecer políticas, medidas e mecanismos adequados para que as entidades se protejam e alcancem um patamar de preparação e maturidade cibernética proporcional às ameaças. Neste domínio, deve ter-se em boa consideração, também, os normativos legais que dispõem sobre a matéria de cibersegurança e a *compliance* com os mesmos, bem como as diretrizes e recomendações de entidades com competência na matéria, como o Centro Nacional de Cibersegurança.

Ademais, e se, por um lado, a digitalização trouxe, também, novos riscos e potenciou o aumento dos ciberataques, por outro lado, existe uma maior conscientização da necessidade de implementar medidas e boas práticas que protejam as entidades no seu todo, incluindo informação, dados, sistemas e recursos e, por conseguinte, a continuidade do seu negócio.

Ainda, e atendendo às próprias interligações entre organizações públicas e privadas, as fragilidades de uma no domínio da cibersegurança podem expor várias outras organizações a ciberameaças, devendo-se, pois, posicionar a cibersegurança como vetor determinante da resiliência das sociedades e organizações como um todo.

A definição de boas práticas fundamentais em matéria de cibersegurança constitui-se como a base de partida para uma estratégia robusta. De igual modo, uma boa governação de cibersegurança é essencial para a segurança da informação e dos sistemas informáticos.

Naturalmente, entre as diversas entidades do setor público e privado existem diferentes níveis de maturidade em matéria de cibersegurança. Assim, propõe-se o desenvolvimento e consolidação de



REGIÃO AUTÓNOMA DOS AÇORES
Presidência do Governo Regional
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

quatro manuais de boas práticas no que concerne à utilização de meios informáticos e de cibersegurança, adaptados, ainda que de forma transversal, às especificidades das entidades.

Neste sentido, o investimento previsto no Plano de Recuperação e Resiliência previsto para a Região Autónoma dos Açores, na sua componente 19 -Transição digital da Administração Pública dos Açores, ao abrigo do Projeto Azores Cyber 360º, engloba o desenvolvimento de manuais de boas práticas de cibersegurança.

Os manuais destinados à APR visam, entre outros, a determinação de políticas e normas de utilização de meios informáticos e a definição de um modelo de governança que permita a gestão e capacidade de resposta adequadas no âmbito da cibersegurança. Enquanto os manuais a serem disponibilizados a entidades terceiras, designadamente PME's e entidades do poder local, visam contribuir para o reforço da maturidade digital e de cibersegurança destas entidades, potenciando o acréscimo da sua resiliência a incidentes e ameaças.

Por conseguinte, o presente procedimento visa a aquisição de serviços de consultoria técnica para o desenvolvimento e consolidação de quatro manuais de boas práticas no que concerne à utilização de meios informáticos e de cibersegurança.

2. Requisitos técnicos

2.1. Na primeira semana de execução deverá ocorrer a sessão de arranque dos trabalhos e o levantamento/mapeamento das especificidades e medidas técnicas e organizativas conducentes à elaboração do Manual de governança, de exploração de sistemas de informação e de cibersegurança da Administração Pública Regional e do Manual do utilizador da Administração Pública Regional de meios informáticos e de cibersegurança. Este levantamento/mapeamento será efetuado pelo cocontratante em articulação com as equipas técnicas da DRCTD.

2.2. O cocontratante obriga-se a desenvolver a prestação de serviços objeto deste procedimento de acordo com o especificado no presente caderno de encargos, resultando na produção de quatro entregáveis com as seguintes especificações, no prazo máximo de 30 dias conforme definido na cláusula 4ª:

I. Manual de governança, de exploração de sistemas de informação e de cibersegurança da Administração Pública Regional

- a. Âmbito e objetivos
- b. Enquadramento legal e compliance
- c. Modelo de governança de IT da APR / responsabilização
- d. Princípios e controlo de segurança da informação e dos dados
- e. Gestão de utilizadores e ciclo de vida
- f. Gestão de ativos
- g. Regras de exploração de sistemas e redes
- h. Desenvolvimento seguro de software
- i. Gestão de fornecedores e prestadores de serviços



REGIÃO AUTÓNOMA DOS AÇORES

Presidência do Governo Regional

DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- j. Cibersegurança:
 - i. Proteção
 - ii. Detecção
 - iii. Resposta e tratamento de incidentes
 - iv. Recuperação
 - v. Comunicação e partilha de informação
 - vi. Gestão do risco e melhoria contínua

II. Manual do utilizador da Administração Pública Regional de meios informáticos e de cibersegurança

- a. Responsabilidades e deveres do utilizador
- b. Boas práticas de utilização de meios informáticos e cibersegurança

III. Manual de boas práticas de cibersegurança para PMEs

- a. Gestão de utilizadores
- b. Responsabilidades e deveres do utilizador
- c. Boas práticas transversais de cibersegurança na ótica do utilizador e na ótica da gestão
 - i. Proteção
 - ii. Detecção
 - iii. Resposta e tratamento de incidentes
 - iv. Recuperação
 - v. Comunicação e partilha de informação
 - vi. Gestão do risco e melhoria contínua

IV. Manual de boas práticas de cibersegurança para freguesias e municípios

- a. Gestão de utilizadores
- b. Responsabilidades e deveres do utilizador
- c. Governança
- d. Boas práticas transversais de cibersegurança na ótica do utilizador e na ótica da gestão
 - i. Proteção
 - ii. Detecção
 - iii. Resposta e tratamento de incidentes
 - iv. Recuperação
 - v. Comunicação e partilha de informação
 - vi. Gestão do risco e melhoria contínua

2.3. Os conteúdos previstos no número anterior são obrigatórios. O concorrente poderá incluir outros conteúdos que considere relevantes, sem prejuízos dos obrigatórios.

2.4. A estrutura de cada manual deverá ser previamente aprovada pela DRCTD em sede de reunião semanal.

2.5. No desenvolvimento dos conteúdos suprarreferidos devem ser considerados, sempre que aplicável, os normativos legais aplicáveis e a informação e recomendações disponibilizadas pelo Centro Nacional de Cibersegurança.