REPÚBLICA DE ANGOLA

Órgãos Auxiliares do Presidente da República

Instituto de Modernização Administrativa

Projecto de Aceleração Digital de Angola

PADA (P180693)

Termos de Referência para Avaliação da Maturidade da Cibersegurança e Desenvolvimento de Estratégias

Luanda, Setembro de 2025

IMA Instituto de Modernização Administrativa

GOVERNO DE ANGOLA

Registo de Versão do Documento

ID. Doc: 01/IMA/2024	**Nome do Projecto:** Projecto de Aceleração Digital de Angola (PADA)
Autor: Instituto de Modernização Administrativa	
Sinopse do Documento: Acelerar a inclusão digital e a adopção de soluções digitais inovadoras para o avanço da economia digital de Angola.	

Versão	Data	Acção	Interveniente	Descrição
1.0	01/10/2025	Criação do Documento	▪ IMA	Elaboração do conteúdo inicial.

Índice

Acrónimos

Sigla	Descrição
CIRT	Computer Incident Response Team
CMM	Cybersecurity Capacity Maturity Model
BM	Banco Mundial
GDA	Governo de Angola
IMA	Instituto de Modernização Administrativa
PADA	Projecto de Aceleração Digital de Angola
PDN	Plano de Desenvolvimento Nacional

1. Contexto

O Governo de Angola (GdA) está a aprofundar a agenda de Transformação Digital da **Administração Pública**, visando modernizar processos, integrar sistemas e melhorar a prestação de serviços aos cidadãos e às empresas. Esta evolução exige que as entidades públicas reforcem, de forma estruturada, a sua capacidade de proteger activos digitais, dados e serviços críticos, assegurando **disponibilidade, integridade e confidencialidade**.

A crescente digitalização e interligação de plataformas e sistemas governamentais, bem como a dependência de fornecedores e prestadores de serviços tecnológicos, ampliam a superfície de ataque e elevam os riscos cibernéticos com impacto directo na continuidade dos serviços públicos. O reforço da cibersegurança na Administração Pública constitui, assim, uma condição essencial para a confiança, resiliência e sustentabilidade das iniciativas de governação digital, com efeitos positivos no ecossistema nacional.

A Lei n.º 15/24 (Lei da Segurança Nacional) posiciona a protecção do ciberespaço como prioridade estratégica, reforçando a necessidade de melhorar a resiliência e confiança nos serviços digitais, com particular incidência nos **activos e infra-estruturas digitais do Estado**.

Apesar de alguns avanços, persistem desafios relevantes na maturidade global da cibersegurança. Torna-se, por isso, necessário adoptar uma abordagem estruturada e faseada para: (i) avaliar risco e capacidades no sector público, (ii) definir Estratégia Nacional de Cibersegurança e Plano de Acção com prioridades para o Estado, e (iii) preparar o desenvolvimento/estabelecimento de uma CIRT nacional com foco primário de suporte à Administração Pública, alinhada com boas práticas e cooperação internacional (ex.: FIRST).

Embora o foco operacional e de implementação desta contratação seja a Administração Pública, os resultados esperados contribuirão, por consequência, para elevar a postura de cibersegurança do ecossistema nacional, através de melhores práticas, referenciais e mecanismos de cooperação e articulação institucional.

2. Descrição Geral do Projecto PADA

O Projecto de Aceleração Digital de Angola - PADA, é uma iniciativa destinada a impulsionar a inclusão digital e a adopção de soluções digitais inovadoras para o avanço da economia digital de Angola. A necessidade do projecto surge do contexto socioeconómico do país, que, apesar de ser uma das maiores economias africanas e um do maioríssimo produtor de petróleo, enfrenta um desafio voltado no crescimento populacional rápido e na necessidade de encontrar soluções para sustentar a demanda existente. O desenvolvimento de uma economia digital tornou-se um pré-requisito para a intenção do Governo de Angola de fazer a transição de uma economia petrolífera para uma economia mais diversificada que possa beneficiar todas as franjas da sociedade, principalmente o cidadão e as empresas. Neste ensejo, a aceleração digital apresenta-se transversalmente como um

catalisador para o desenvolvimento em vários sectores. Considerando essas observações, o Governo de Angola, com recurso ao financiamento e assistência do Banco Mundial, aprovou a implementação do PADA.

O PADA resulta da necessidade de materialização da Agenda de Transição Digital da Administração Pública, subordinada ao Plano Nacional de Desenvolvimento até 2027, que assenta essencialmente na adopção **Administração Digital e Interoperável**, alinhada ao Roteiro para a Reforma do Estado, ao Roteiro para a Transição Digital da Administração Pública e à Arquitectura Global para a Interoperabilidade da Administração Central e Local do Estado.

Sob coordenação do Instituto de Modernização Administrativa – IMA, o PADA foi desenhado com base nos estudos e nas missões realizadas pela equipa do Banco Mundial e a participação dos demais órgãos do sector público. Fruto das missões do Banco Mundial em Angola, foi realizado o Diagnóstico para a Economia Digital de Angola - DE4A, apresentado no Fórum IMA a 03 de Março de 2022. O Diagnóstico apresentou como solução aos desafios identificados, a necessidade de fortalecer o ecossistema digital por meio da implementação de plataformas digitais, acesso a serviços digitais, reformas legais e criação de competências para a sociedade.

O PADA tem uma duração de cinco (5) anos com um financiamento de USD 300.000.000 (trezentos milhões de dólares americanos), com foco em cinco (5) componentes, sendo três (3) componentes de implementação de projectos e duas (2) componentes de gestão:

1. Componente 1: Programa de Inclusão Digital de Acesso Universal;
2. Componente 2: Expansão da infra-estrutura pública digital inclusiva e segura;
3. Componente 3: Oportunidades Digitais para a Diversificação Económica;
4. Componente 4: Gestão de Projectos;
5. Componente 5: Componente de Resposta de Emergência Contingente.

A. Visão geral

O Governo de Angola em parceria com o Banco Mundial, dará resposta aos desafios da exclusão digital, ineficiência dos serviços públicos e oportunidades económicas limitadas, através do PADA. Com um envolvimento multissectorial, com actividades que se reforçam mutuamente e que estão alinhadas com as prioridades e planos do Governo, o PADA visa desbloquear a aceleração digital do país e, ao mesmo tempo, apoiar nas agendas sobrepostas de alívio da pobreza, diversificação económica e modernização da prestação de serviços públicos. O PADA prevê três componentes para enfrentar os desafios acima mencionados e alcançar o propósito descrito.

B. Objectivos de Desenvolvimento do Projecto

Os objectivos de Desenvolvimento do Projecto são o de acelerar a inclusão digital, aumentar o acesso a serviços habilitados digitalmente e conceder oportunidades digitais para o avanço da economia digital de Angola.

C. Beneficiários do Projecto

O PADA visa beneficiar toda a população angolana, mas particularmente aquelas que actualmente se encontram excluídas digitalmente.

O público-alvo do PADA inclui:

1. **Cidadãos:** O projecto visa melhorar o acesso da população aos serviços digitais, promover a inclusão digital, e garantir que comunidades mais remotas também tenham acesso a recursos como internet de banda larga e tecnologias de informação, fornecer a identidade digital aos cidadãos permitindo-lhes o acesso aos serviços públicos, apoios governamentais e serviços financeiros, não carecendo a identidade pessoal e formal (bilhete de identidade) e assim elevar a segurança dos pagamentos electrónicos

2. **Empresas e Empreendedores:** Pequenas e médias empresas (PMEs) e start-ups são um foco importante, com o objectivo de impulsionar o desenvolvimento de negócios baseados em tecnologia e inovação. O projecto oferece suporte ao crescimento de novos modelos de negócios digitais.

3. **Administração Pública:** Outro público-alvo são os órgãos governamentais, com o objectivo de modernizar os serviços públicos, melhorar a eficiência e facilitar o acesso dos cidadãos a esses serviços através de plataformas digitais.

4. **Estudantes e Profissionais de TIC:** O PADA também visa facilitar a capacitação de estudantes e profissionais na área de tecnologia da informação e comunicação (TIC), oferecendo oportunidades de treinamento e desenvolvimento de habilidades digitais

D. Estrutura Global do Projecto

As componentes do PADA correspondem ao conjunto de actividades e projectos que devem ser realizados para a implementação prática do Projecto. As componentes estão divididas por

subcomponentes que contém o conjunto de projectos e actividades. Cada componente do projecto tem atribuída um valor para a implementação desses projectos e actividades identificados.

- **Componente 1 - Programa de Inclusão Digital de Acesso Universal:** Esta componente centra-se na expansão de infra-estruturas e serviços de banda larga essenciais, de alta qualidade, resilientes e acessíveis, enquanto apoia o investimento em infra-estruturas de dados seguras e o desenvolvimento de mercados de cloud e de alojamento de dados. As actividades no âmbito deste pilar visam fortalecer as instituições e ajudar a impulsionar o investimento privado em redes de telecomunicações e instalações de alojamento de dados, que são bases fundamentais para a utilização produtiva de tecnologias e dados digitais.

- **Componente 2 - Expansão de infra-estrutura pública digital inclusiva e segura:** Esta componente centrar-se-á na implantação de infra-estrutura pública digital, na criação de mecanismos interoperáveis para aumentar a eficiência nos sectores público e privado, fortalecendo as instituições públicas e desenvolvendo os facilitadores transversais e as salvaguardas digitais necessárias para promover a utilização confiável e segura das tecnologias digitais e dos serviços digitalmente habilitados a nível nacional e além fronteiras, bem como garantindo aos cidadãos "visibilidade" assente numa identidade segura, facilmente verificável pelos sectores publico e privado, e cuja utilização seja um agregador de valor.

- **Componente 3 - Oportunidades Digitais para a Diversificação Económica:** Ampliar a capacidade das start-ups, por meio de financiamentos e capacitação de habilidades digitais para empreendedores.

O PADA conta com três (3) indicadores que são:

I. Aumentar o acesso universal à Internet de banda larga, que visa aumentar o número de pessoas a utilizar a internet de banda larga de 14.743.807 para 19.700.000 até Março de 2030.

II. Aumentar o acesso a serviços públicos de alto impacto, para prover uma identidade digital até 10.000.000 de pessoas até Março de 2030.

III. Aumentar o acesso a oportunidades digitais relevantes para o sector do empreendedorismo, por aumentar o número de empresas que adoptaram produtos tecnológicos para oferecer serviços de raiz digital até 400 empresas em Março de 2030

E. Disposições Institucionais e Responsabilidades

Para a implementação do PADA, o Governo de Angola é representado pelo IMA, na qualidade de órgão central do aparelho do Estado que tem por missão elaborar e implementar as medidas de política de suporte à Modernização Administrativa, conceber e implementar o modelo de alinhamento entre a Governação Pública e a Governação Electrónica.

Na qualidade de Unidade de Implementação do PADA (UIP), o IMA é responsável pela implementação geral e coordenação diária do Projeto, incluindo: gestão financeira e aquisições, monitoramento e avaliação das actividades do Projeto, gestão ambiental e social.

3. Objectivos da Contratação

Contratar uma consultoria devidamente qualificada para **avaliar o risco e a maturidade/capacidade de cibersegurança no sector público (Administração Pública)**, desenvolver a Estratégia Nacional de Cibersegurança e o respectivo Plano de Acção com medidas prioritárias para o reforço da segurança dos serviços e activos digitais do Estado, e avaliar a prontidão e definir o plano para o desenvolvimento/estabelecimento de uma CIRT nacional **com mandato e foco primário de suporte à Administração Pública**, no contexto do PADA, assegurando efeitos positivos e alinhamento com o ecossistema nacional.

Objectivos Especificos:

i. Realizar uma avaliação nacional de cibersegurança identificando as principais lacunas e fornecendo recomendações prioritárias.
ii. Realizar uma avaliação de cibersegurança **centrada na Administração Pública**, identificando lacunas, riscos e prioridades de mitigação nos serviços, dados e infra-estruturas digitais do Estado, incluindo dependências críticas (fornecedores e prestadores).
iii. Desenvolver a Estratégia Nacional de Cibersegurança e um Plano de Acção faseado, com **medidas prioritárias para o sector público**, incluindo custos, responsabilidades institucionais e mecanismos de execução.
iv. Avaliar o nível de preparação e definir um plano para o desenvolvimento/estabelecimento de uma CIRT nacional **orientada à protecção e resposta a incidentes na Administração Pública**, incluindo serviços, público-alvo, recursos, roteiro e documentação para concurso, assegurando capacidade de articulação com actores nacionais relevantes quando aplicável.
v. Incorporar boas práticas amplamente aceites para permitir participação em iniciativas e fóruns de cooperação internacional (ex.: FIRST), reforçando a capacidade de resposta e coordenação do Estado.

Os serviços de consultoria serão financiados ao abrigo do projecto e o Contracto de Serviços de Consultoria será gerido pela UIP.

4. Descrição do Trabalho e Considerações Metodológicas

A empresa de consultoria ("Consultor") utilizará uma abordagem faseada, com base em quadros metodológicos reconhecidos internacionalmente (nomeadamente o Modelo de Maturidade Cibernética (CMM, na sigla em inglês), o Guia para o Desenvolvimento de uma Estratégia Nacional de Cibersegurança, o NIST, NCRA, ITU CIRT Readiness Assessment, ENISA CSIRT Establishment etc.).

Mais especificamente, espera-se que o Consultor realize as seguintes actividades:

Actividade 1 — Planeamento e instalação da execução

1. Definir mecanismos de governação da actividade, em colaboração com o IMA/UIP e sob orientação dos Comités Director e Técnico do PADA.
2. Identificar partes interessadas e desenvolver plano/matriz de envolvimento (Governo, sector privado, sociedade civil, academia), com foco nos intervenientes relevantes para a **Administração Pública**.
3. Desenvolver plano do projecto (tarefas, etapas, partes envolvidas).
4. Considerar modelos de colaboração (Governo, reguladores, operadores, seguradoras) para soluções inovadoras (ex.: seguros cibernéticos) quando relevantes para a continuidade e mitigação de riscos nos serviços públicos.

Actividade 2 — Avaliação de risco cibernético e capacidades nacionais (maturidade)

1. Realizar avaliação aprofundada de risco e capacidades, usando referenciais reconhecidos (ex.: NIST, NCRA, COBIT, CMM), com prioridade no **sector público**.
2. Incluir alinhamento com normas/conformidades internacionais (ex.: PCI-DSS, ISO/IEC 27001) para recomendações específicas, quando aplicáveis ao contexto e dependências da Administração Pública.
3. Considerar aplicação do NIST CSF e boas práticas para infra-estruturas críticas (OT/ICS) com incidência em serviços e activos do Estado.
4. Integrar metodologias de Third-Party Risk Management (TPRM) na análise de riscos, **com enfoque nas dependências críticas da Administração Pública**, incluindo fornecedores, operadores e prestadores relevantes, nomeadamente nos sectores financeiro e telecomunicações quando impactem serviços públicos e infra-estruturas do Estado.
5. Utilizar, quando aplicável, ferramentas de avaliação contínua (ex.: SecurityScoreCard) para acompanhar a postura de segurança de **fornecedores e parceiros estratégicos que suportem serviços públicos**.
6. Preparar missão: metodologia, logística, instrumentos de recolha (questionários/entrevistas), lista ideal de organizações e requisitos de workshops.
7. Realizar workshop de consulta (5 dias) e recolher dados necessários para análise e revisão do risco e capacidade de cibersegurança, com prioridade em actores da Administração Pública e dependências críticas.
8. Executar controlo de qualidade e colmatar lacunas por pesquisa documental e sessões de seguimento.
9. Produzir projecto de relatório CMM e relatório de avaliação de risco, com recomendações revistas por pares e priorizadas para o sector público.
10. Facilitar workshop de validação e produzir versões finais incorporando feedback.

Actividade 3 — Estratégia Nacional de Cibersegurança + Plano de Acção

1. Definir prioridades e objectivos estratégicos com base nos relatórios da Actividade 2 e

consultas às partes interessadas, assegurando **priorização de medidas para a Administração Pública**.

2. Elaborar Estratégia Nacional de Cibersegurança e preparar versão final para aprovação governamental.
3. Construir Plano de Acção orçamentado e priorizado, faseado, incluindo iniciativas com implementação prioritária no sector público, e preparar versão final para aprovação.
4. Preparar até 6 mandatos (incluindo especificações técnicas e documentação preliminar de concurso) para actividades relevantes do Plano de Acção, incluindo: protecção de infra-estruturas críticas; protecção de serviços de e-governance; capacidades de resposta a incidentes; sensibilização e competências; harmonização do quadro jurídico e protecção de dados com boas práticas regionais e internacionais.

Actividade 4 — Avaliação de prontidão e Plano de desenvolvimento/estabelecimento da CIRT

A avaliação e o plano de CIRT deverão considerar uma CIRT nacional com **mandato, governação e capacidade operacional prioritariamente orientados à Administração Pública**, assegurando mecanismos de articulação e cooperação com sectores nacionais relevantes quando necessário.

1. Preparar avaliação no local: estudos e análise das capacidades actuais; identificação de dados/documentos e partes interessadas.
2. Realizar workshops/interacções e entrevistas para avaliar necessidades, lacunas e remediações.
3. Elaborar Relatório de Avaliação de Prontidão, incluindo: capacidades existentes; mandato preliminar; governação; requisitos de alojamento; roteiro e orçamento de alto nível; requisitos para fase de projecto.
4. Elaborar Plano de Estabelecimento/Desenvolvimento da CIRT, incluindo: mandato detalhado; serviços; processos/fluxos; organização/competências/formação; instalações; tecnologias e automação; cooperação; gestão de TI e segurança; roteiro detalhado; editais de licitação para implementação.
5. Incluir exercícios práticos e simulações como parte da preparação da CIRT.
6. Elaborar planos de continuidade de negócios e resposta a incidentes adaptados a sectores críticos, priorizando a continuidade de serviços públicos.

Actividade 5 — Workshop de formação (3 dias)

1. Desenvolver módulos de formação baseados em princípios e boas práticas de cibersegurança, incluindo aspectos e procedimentos políticos da Estratégia Nacional, com enfoque na aplicação prática no sector público.
2. Adaptar formação às necessidades/objetivos específicos de Angola e personalizar conteúdos.
3. Realizar sensibilização para riscos e melhores práticas.
4. Ministrar formação prática sobre desenvolvimento de políticas, com ferramentas e exemplos.
5. Facilitar discussões e partilha de experiências para aprendizagem colaborativa.
6. Considerar formação contínua e sensibilização em higiene digital e parcerias para certificação sectorial (quando aplicável).

5. Responsabilidade da UIP

O Governo de Angola deverá fornecer o seguinte, da melhor forma possível:

- Todos os dados de base e literatura considerados relevantes para realizar ou informar a tarefa e completar as tarefas identificadas à sua disposição imediata.
- Acesso a funcionários-chave dos ministérios/agências/departamentos relevantes e outras entidades oficiais relevantes, conforme aplicável.
- Facilitar a cooperação de outras organizações, cujas actividades e programas possam ser considerados relevantes para a atribuição.
- Outro apoio logístico, conforme necessário.

6. Duração do Contrato

Duração do Contracto: Prevê-se que a duração do contracto seja de quatro (4) meses, equivalente a 16 semanas.

7. Entregáveis do Contrato

Entregável	Prazo	Pagamento (%)
E1 Relatório inicial (Inception), plano de execução, governação, metodologia e plano de consultas	1 semana após assinatura	10%
E2 Relatório de avaliação de risco + maturidade/capacidade (CMM)	4 semanas após assinatura	30%
E3 Estratégia Nacional de Cibersegurança + Plano de Acção	8 semanas após assinatura	20%
E4 Relatório de prontidão + Plano de desenvolvimento/estabelecimento da CIR	12 semanas após assinatura	20%
E5 Pacote de TdRs/mandatos (até 6) + documentação preliminar de concurso	14 semanas após assinatura	10%
E6 Workshop de formação (3 dias) + materiais e evidências	15 semanas após assinatura	5%
E7 Relatório final consolidado + consolidação de evidências, lições aprendidas e handover	16 semanas após assinatura	5%*

8. Comunicação e Reporting

Requisitos de *Reporting:* O Consultor deverá assegurar que os entregáveis devem ser submetidos a UIP do PADA, os documentos produzidos devem ser escritos em português e submetidos electronicamente em formato PDF e Word editável, permitindo a realização de comentários/edições. Adicionalmente deverá submeter para cada entregável uma apresentação em *powerpoint* com o resumo do conteúdo dos mesmos.

A UIP do PADA será responsável pela revisão de cada entregável, e reservará uma (1) semana para fornecer feedback/validar cada entregável. Mediante solicitação, o Consultor também pode ser solicitado a apresentar os resultados verbalmente (pessoalmente ou virtualmente) às partes interessadas para permitir feedback e validação.

1. Localização

A empresa seleccionada deve estar disponível para trabalhar em Angola (por exemplo, através de missões no terreno), uma vez que tal facilitará a recolha dos contributos necessários, o conhecimento do contexto local e também apoiará uma transferência de conhecimentos mais eficaz.

2. Transferência de Conhecimento

A transferência de conhecimento é considerada parte integrante desta tarefa e deve reflectir-se na metodologia do consultor e na proposta técnica. Idealmente, o Governo deve ser capaz de aprender a replicar/actualizar elementos-chave da atribuição, se necessário, no futuro.

3. Requisitos de Qualificação

A empresa seleccionada terá de demonstrar as seguintes qualificações:

- Possuir fortes competências e experiência em cibersegurança e Tecnologias da Informação e Comunicação (TIC), nomeadamente nas seguintes áreas: governação, legislação, gestão de riscos, protecção de infra-estruturas críticas de informação, resposta a incidentes e desenvolvimento de competências em cibersegurança, com pelo menos 5 anos de experiência relevante.
- Amplo conhecimento da política, estratégia e operações de cibersegurança em contexto governamental.
- Uma metodologia adequada e experiência na aplicação de ferramentas de investigação relacionadas.
- Ter realizado pelo menos 2 (duas) missões semelhantes, preferencialmente em Países Africanos.
- Demonstrar uma compreensão das principais estruturas, metodologias e melhores práticas em cibersegurança, incluindo: Guia para o desenvolvimento de uma estratégia nacional de cibersegurança, CMM (Capability Maturity Model), NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), ISO 2700x, etc.

- É preferível ter experiência prévia de trabalho com o sector público.
- A experiência no contexto de um país em desenvolvimento é considerada uma vantagem.

A empresa deve propor uma equipa principal composta, no mínimo, por um chefe de equipa, (2) peritos técnicos, além de todo o pessoal de apoio adicional considerado necessário para executar o trabalho. Se os membros da equipa não forem fluentes em português, terá de ser contratado um tradutor simultâneo de português para garantir uma comunicação eficaz. Sendo o português a língua oficial de Angola, a capacidade de trabalhar em português é uma vantagem.

A empresa de consultoria deve fornecer um plano de pessoal com nomes, funções e currículos para a equipe principal do projeto como parte da proposta.

Posição-chave	Experiência	Qualificações
(1) Chefe de Equipa, ou equivalente	Mínimo de 7 anos de experiência na indústria de cibersegurança Experiência na liderança de projectos de cibersegurança e conhecimento das melhores práticas globais no desenvolvimento de políticas de cibersegurança. Excelente capacidade de comunicação e liderança, e experiência na gestão de projectos complexos Experiência anterior e networking e colaboração com instituições governamentais.	Mestrado em Ciência da Computação, Cibersegurança, Ciência/ Tecnologia e/ou outras áreas relevantes.
(1) Política de cibersegurança ou especialista em governação	Pelo menos 5 anos de experiência em política e governança de segurança cibernética, com foco em políticas, regulamentações e normas de segurança cibernética de nível nacional. Capacidade comprovada de conceber e implementar políticas e regulamentos de cibersegurança e de assegurar a conformidade com normas e regulamentos nacionais e internacionais relevantes.	Mestrado em Cibersegurança/ Segurança da Informação, Negócios/ Administração Pública, Economia, Estudos de Desenvolvimento, Comércio, Ciência/ Tecnologia, ou outras áreas relevantes.

	Conhecimento dos requisitos legais e regulamentares relevantes, tais como regulamentos de protecção de dados, legislação de uso indevido de computadores e políticas de protecção de infra-estruturas críticas	
(1) Especialista em Gestão de Riscos e CIIP	Pelo menos 5 anos de experiência em gestão de riscos e PICI, preferencialmente a nível nacional. Conhecimento aprofundado de gestão de riscos e estruturas CIIP, como NIST SP 800-53, ISO/IEC 27001 ou CIP-014-1, e sua aplicação aos processos de protecção CII. Certificações relevantes, como Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) ou Certified Critical Infrastructure Protection Professional (CCIPP), são altamente desejáveis.	Mestrado em Cibersegurança/ Segurança da Informação, Negócios/ Administração Pública, Economia, Estudos de Desenvolvimento, Comércio, Ciência/ Tecnologia, ou outras áreas relevantes.
(1) Especialista em Resposta a Incidentes	Pelo menos 5 anos de experiência em resposta a incidentes de cibersegurança, com foco no estabelecimento e gestão de CIRTs Conhecimento aprofundado das estruturas e metodologias de estabelecimento de RI e CIRT, como a estrutura de serviço FIRST, NIST SP 800-61, ISO/IEC 27035, SANS Incident Handling Guidelines, e sua aplicação à construção e operação de CIRTs eficazes. Capacidade comprovada de projetar e implementar políticas, procedimentos e fluxos de trabalho de resposta a incidentes, e de treinar e orientar os membros do CIRT sobre as melhores práticas de resposta a incidentes. Certificações relevantes, como Certified Information Systems Security Professional	Mestrado em Cibersegurança/Segurança da Informação, Negócios/ Administração Pública, Economia, Estudos de Desenvolvimento, Comércio, Ciência/ Tecnologia, ou outras áreas relevantes.

	(CISSP), GIAC Certified Incident Handler (GCIH) ou ECIH Certified Incident Handler (ECIH), são altamente desejáveis.	
(1) Especialista em desenvolvimento de competências em cibersegurança	Pelo menos 5 anos de experiência no desenvolvimento de competências de cibersegurança Capacidade comprovada de projetar e fornecer programas de treinamento em segurança cibernética, incluindo desenvolvimento curricular, design instrucional e entrega de cursos. Familiaridade com várias ferramentas e técnicas de treinamento em segurança cibernética, como simulações, exercícios práticos e plataformas de treinamento on-line.	Mestrado em Cibersegurança/ Segurança da Informação, Negócios/ Administração Pública, Economia, Estudos de Desenvolvimento, Comércio, Ciência/ Tecnologia, ou outras áreas relevantes.

9. Código de Conduta

- Actuar com honestidade, transparência e respeito em todas as actividades.
- Evitar conflitos de interesse e agir de maneira a promover o bem-estar colectivo.
- Proteger informações confidenciais e sensíveis, garantindo que apenas pessoas autorizadas tenham acesso a elas.
- Não divulgar ou utilizar informações privilegiadas para ganho pessoal ou de terceiros.
- Cumprir prazos e compromissos acordados, garantindo a qualidade e a entrega dos resultados.
- Assumir responsabilidade por acções e decisões, e comunicar problemas ou dificuldades de forma proactiva.
- Obedecer às leis, regulamentos e políticas internas aplicáveis ao trabalho.
- Garantir que todas as actividades e decisões estejam alinhadas com as normas éticas e legais vigentes.
- Buscar constantemente o aprimoramento profissional, mantendo-se actualizado sobre as melhores práticas e inovações na área de actuação.

- Demonstrar comprometimento com a qualidade e a excelência em todas as tarefas e projectos.

10. Confidencialidade e Segurança da Informação

Para garantir a confidencialidade das informações tratadas durante a execução do projecto, as seguintes medidas deverão ser adoptadas:

1) Acordo de Confidencialidade (NDA): Todos os membros da equipa de consultoria deverão assinar um Acordo de Confidencialidade (*Non-Disclosure Agreement* - NDA), comprometendo-se a manter sigilo sobre todas as informações sensíveis e estratégicas a que tiverem acesso durante o projecto.
2) Cláusulas Contratuais de Confidencialidade: O contrato de prestação de serviços incluirá cláusulas específicas que determinem a obrigação de manter a confidencialidade de todas as informações obtidas, incluindo dados pessoais, estratégias governamentais, informações técnicas e operacionais.
3) Regras para Transferência de Dados: Qualquer transferência de dados entre a consultoria e o Governo deverá ser realizada por canais seguros e institucionais/oficiais, assegurando que os dados sensíveis não sejam expostos a riscos durante o processo.

11. Candidaturas

Os candidatos interessados devem fornecer informações que indiquem que estão qualificados para a realização dos serviços e são convidados a apresentar a sua candidatura mediante a apresentação dos seguintes documentos:

- Carta de manifestação de interesse com dados e documentos da empresa que comprovam a sua capacidade;
- Proposta Financeira;
- Proposta de trabalho;
- Curriculum Vitae dos especialistas.

Os interessados poderão submeter as suas candidaturas na data de publicação do concurso para o endereço indicado no comunicado do anúncio do concurso.