Termos de Referência

CONTRATAÇÃO DE UMA ENTIDADE PARA FORMAÇÃO E CERTIFICAÇÃO INTERNACIONAL EM SEGURANÇA CIBERNÉTICA

JULHO DE 2019

INDÍCE

I. PREÂMBULO **3**

II. FINALIDADE DO TERMO DE REFERÊNCIA **3**

Objectivo Geral ..... Error! Bookmark not defined.

Objectivo específico ..... Error! Bookmark not defined.

III. RESPONSABILIDADES DAS PARTES **9**

Deverá entidade contratante: **9**

O (a) contratado(a) deverá: **9**

Forma de Contratação **10**

Prazo e entregáveis **10**

Produto ..... Error! Bookmark not defined.

Perfil da Empresa **10**

Processo de candidatura **11**

IV. ESPECIFICAÇÕES TÉCNICAS ..... Error! Bookmark not defined.

De Serviços ..... Error! Bookmark not defined.

Do Sistema ..... Error! Bookmark not defined.

Funcionalidade de base da plataforma ..... Error! Bookmark not defined.

V. PAGAMENTO **12**

I. PREÂMBULO

Moçambique partilha com muitos outros países a necessidade de se saber quais são as organizações que maior a confiança merecem dos cidadãos e que mais respeitam os princípios de boa conduta e de ética, sob vários pontos de vista.

Neste sentido, o Índice de Transparência que a OCAM pretende construir é o primeiro, uma vez que será publicado sob-forma de ranking nacional, com diversas categorias, designadamente: microempresas, pequenas, médias e grandes empresas ou organizações da sociedade civil.

Entretanto, nenhum índice foi, até hoje, elaborado para classificar a transparência das ISCE (Instituições da Sociedade Civil e Empresarial), pois as empresas privadas com fins lucrativos têm sido o alvo, ao passo que, neste caso, o foco assenta nas organizações da sociedade civil e, apenas, numa segunda fase, nas empresas privadas.

A OCAM, na sua estratégia de desenvolvimento, estabelece actividades que visam o desenvolvimento e transparência da sociedade civil no país. Para conseguir concretizar os seus objectivos pretende "medir" a transparência das instituições da sociedade Civil e do Sector Empresarial em que é um conceito complexo e vai muito além do simples aspecto contabilístico, alastrando-se aos demais elementos das ISCE de Moçambique.

II. FINALIDADE DO TERMO DE REFERÊNCIA

Decorrente da crescente globalização dos mercados e, por via disso, de uma maior exigência na racionalização, organização e rapidez das empresas, a externalização das actividades produtivas e/ou distributivas tem aumentado. É, pois, vital compreender a importância da ligação com o meio transacional a montante e a jusante na cadeia

logística, bem como, reconhecer a importância do *segurança de redes* e dos aspetos mais relevantes associados à negociação e posterior contratação de bens e/ou serviços de informática.

OBJETIVOS

- Dar a conhecer e compreender as estruturas actuais no mercado que podem ser usadas para apoiar a implementação de um programa de segurança cibernética;
- Aplicar mecanismos para operacionalizar um programa e estrutura se segurança cibernética.
- Apoio na identificação e aplicação de controles de segurança cibernética para mitigar riscos e evitar violações de segurança.
- Compreender os princípios fundamentais de auditoria para prestar apoio na auditoria de programas e estrutura de segurança cibernética.

Objectivo Geral

O objectivo deste documento é estabelecer condições para contratação de uma entidade especializada em prestação de serviços e consultoria em tecnologias de informação para ministrar uma formação à OCAM em Cyber Security (Segurança Cibernética), no que tange a solução de serviços de segurança computacioanal e governança de dados para ambiente heterogêneo, com certificação internacional ISO/IEC 27001.

Objectivos específicos

No final os colaboradores devem ter o conhecimento e o seguinte perfil:

- Manter-se actualizado com os mais recentes desenvolvimentos de segurança e tecnologia.

- Pesquisar / avaliar ameaças emergentes de segurança cibernética e formas de gerenciá-las
- Planejar a recuperação de desastres no caso de qualquer violação de segurança
- Monitorar ataques, intrusões e atividades incomuns, não autorizadas ou ilegais
- Testar e avaliar produtos de segurança
- Projetar novos sistemas de segurança ou atualizar os já existentes
- Usar ferramentas analíticas avançadas para determinar padrões e vulnerabilidades emergentes
- Envolver-se em 'hacking ético', por exemplo, simulando violações de segurança
- Identificar possíveis fraquezas e implementar medidas, como firewalls e criptografia.
- Investigar alertas de segurança e fornecer resposta a incidentes.
- Monitorar o gerenciamento de identidade e acesso, incluindo o monitoramento de abuso de permissões por usuários autorizados do sistema
- Estabelecer contacto com as partes interessadas em relação a questões de segurança cibernética e fornecer recomendações futuras.
- Gerar relatórios para o pessoal técnico e não técnico e partes interessadas
- Manter um registro de riscos à segurança da informação e auxiliar nas auditorias internas e externas relacionadas à segurança da informação.
- Monitorar e responder a e-mails de phishing e atividades "pharming"
- Ajudar na criação, manutenção e entrega de treinamento de conscientização de segurança cibernética para colegas.
- Dar conselhos e orientações à equipe sobre questões como spam e e-mails indesejados ou mal-intencionados.

PROGRAMA

O programa de formação em segurança cibernética deve baseiar-se nos seguintes módulos:

I. **CompTIA Cybersecurity Analyst**

II. **CompTIA PenTest+ (Ethical Hacking)**

III. **CompTIA Advanced Security Practitioner**

CONTEÚDOS ESPECÍFICOS

Fundamentos de Segurança e Informática

- Introdução à temática da segurança.
- Evolução e antecedentes históricos
- Panorâmica geral sobre a atual
- Hardware
- Sistemas Operativos
- Virtualização e Cloud Computing
- Criação de máquinas virtuais no Hyper-V e Virtual Box
- Utilização prática dos dois hipervisores
- Criptografia
- Senhas
- Redes de computadores

Fundamentos de Segurança (e-Learning)

- Noções básicas sobre camadas de segurança;
- Autenticação, Autorização e Contabilidade;
- Noções Básicas Sobre Políticas De Segurança;
- Noções básicas sobre segurança de rede;

- Protegendo o servidor e o cliente;
- CompTIA Security;
- Fundamentos de segurança;
- Segurança de dados;
- Segurança de Aplicativos;
- Proteção de hosts e dispositivos;
- Proteção de Rede Interna;
- Segurança física;
- Conformidade e segurança operacional;
- Ameaças;

Hacking Ético

- Introdução ao Hacking Ético;
- Footprinting e reconhecimento;
- Redes de Digitalização;
- Detenção e análise de vulnerabilidades;
- Sistema de Hacking;
- Ameaças de malwar;e
- Sniffing;
- Negação de serviço;
- Sequestro de Sessão;
- Evading IDS, Firewalls e Honeypots;
- Hackeamento de Servidores Web;
- Aplicativos da Web de hackers;
- SQL Injection;
- Wireless Hacking;

- Hacking de plataformas móveis;
- IoT Hacking;
- Cloud Computing;
- Criptografia;
- Serviços de Teste de Penetração Ofensiva;
- Capturando o tráfego;
- Ataques por senha;
- Exploração do lado do cliente;
- Social Engineering;
- Teste de aplicativos da web;
- Ataques wireless;

Gestão de Segurança da Informação ISO / IEC 27001/27002

- Introdução à família de normas ISO 27000 Introdução aos sistemas de gestão e abordagem de processos;
- Requisitos gerais da ISO / IEC 27002;
- Fases de implementação da estrutura ISO / IEC 27002;
- Introdução ao gerenciamento de riscos de acordo com a ISO 27005;
- Melhoria contínua da segurança da informação;
- Realizando uma auditoria de certificação ISO / IEC 27002;

Proteção de Dados (Segurança de Sistemas de Informação)

- Segurança e Gestão de Riscos;
- Segurança de Activos;
- Engenharia de Segurança;

- Comunicações e Segurança de Redes;
- Gestão de Identidades e Acessos;
- Avaliação de Segurança e Testes;
- Operações de Segurança;
- Segurança em Desenvolvimento de Software

METODOLOGIA

A formação em **Segurança Cibernética** deve ser presencial e baseado em sessões teóricas e práticas com:

- Palestras ilustradas com exemplos baseados em casos reais.
- Exercícios práticos baseados em um estudo de caso completo.

III. RESPONSABILIDADES DAS PARTES

Deverá entidade contratante:

1. Colaborar com a entidade, prestando-lhe todas as informações de que disponha e que, tendo em conta as circunstâncias, se mostrarem necessárias para a boa execução do contracto.

O (a) contratado(a) deverá:

1. Deve ter uma experiência de 5 anos ou mais no ramo com o conhecimentos sólidos e facultar o uso na plataforma;
2. Orientação e ferramentas de apoio para qualquer autoridade sobre como implantar Compras Sustentáveis e inovação na prática – independente de seu tamanho ou nível de experiência.

Forma de Contratação

O presente serviço será contratado mediante a fixação do preço fixo.

Prazo e entregáveis

O prazo de vigência do contrato será de 15 dias e a prestação de serviços terá o seu início no mês de Agosto.

Perfil da Empresa

A empresa deve reunir os seguintes requisitos:

- Registo na conservatória do registo comercial, com licença para prestação de serviços no ramo das tecnologias de informação, com pelo ou menos 5 anos de experiênica na actuação nas áreas de Formação, Educação e Serviços Profissionais, potenciados por Tecnologias de Informação.
- Ter experiência comprovada por meio de cartas abonatórias de capacidade técnica na prestação de serviços em formação em Segurança Cibernética e Certificação.
- A entidade deve ser especializada em fornecer soluções de formação, capacitação e certificação com formador autorizado pelo forncedor (Parceiro).
- Deve apenas fazer uso apenas de material de curso autorizado pelo fornecedor, formadores certificados e instalações de laboratório que excedam as especificações internacionais conforme determinado por cada fornecedor (Parceiro).
- Possuir instalações de formação de última geração e ter reconhecimento pelo compromisso em fornecer (Parceiro) os mais altos níveis de qualidade de soluções e ou serviços.

Processo de candidatura

Para candidatar-se ao concurso, todos(as) os(as) candidatos(as) deverão enviar os seguintes documentos:

a) Comprovativos de registo comercial e as respectivas licenças;
b) Quitação das Finanças, do INSS e Tribunal;
c) Proposta Técnica e Financeira;

Todos os documentos não originais deverão estar devidamente autenticados pela entidade competente. O Concorrente apresentará relação de Trabalhos Similares realizados para outras entidades e/ ou empresas, de preferência em Moçambique e de dimensão semelhante.

Para cada uma das referências deverá ser indicada:

- Nome do Cliente;
- Sector de actividade;
- Período (datas de início e fim de realização do projecto);
- Descrição do Trabalho realizado;
- Contacto privilegiado do Cliente;
- Carta abonatória (desejável);

Os candidatos deverão submeter os documentos acima exigidos para o seguinte endereço:

Ordem dos Contabilistas e Auditores de Moçambique (OCAM)

Rua Projectada à Base T'Chinga 1383, 1ª Rua Perpendicular nº 26

Bairro da Coop,

Distrito Municipal Ka m'pfumu

Cidade de Maputo - Moçambique

As candidaturas deverão ser enviadas até ao **dia 25 de Julho de 2019**, pelas 16:00 horas. Não serão aceites candidaturas recebidas após esta data.

Somente os candidatos selecionados serão contactados.

IV. PAGAMENTO

O consultor/empresa deve apresentar um orçamento, descriminando, honorários, despesas reembolsáveis e impostos.

- Os pagamentos serão feitos em 3 moldes: 40% no acto de adjudicação, 30% após a apresentação da 1ª fase da base de dados e os restantes pagos após a aprovação da base de dados funcional e os documentos finais e aprovados pela OCAM.

O consultor/empresa interessado deverá fazer uma proposta técnica e financeira.