

c

**TERMOS DE REFERÊNCIA PARA A PRODUÇÃO DE MATERIAl PARA CAMPANHA DE SEGURANÇA DIGITAL**

**Termos de Referência**

1. **INTRODUÇÃO**

Em outubro de 2024, Moçambique realizará as suas sétimas eleições gerais, durante as quais serão escolhidos o próximo Presidente da República, os membros da Assembleia da República, os Governadores Provinciais e os membros das Assembleias Provinciais. As eleições gerais anteriores, realizadas no ano de 2019, foram marcadas por graves episódios de violência contra Defensores de Direitos Humanos e por abusos significativos desses direitos. Além disso, entre as eleições gerais de 2019 e as de 2024, ocorreram as sextas eleições autárquicas, também caracterizadas por um ambiente de extrema violência contra DDH, incluindo detenções arbitrárias, ataques físicos, ameaças e a apreensão de equipamentos de trabalho, como computadores e telefones celulares.

No entanto, esse cenário não é exclusivo de Moçambique, ele reflete um panorama mais amplo de repressão do espaço cívico em toda a África, onde DDH enfrentam constante perseguição e ataques cibernéticos. A repressão e a censura crescentes manifestam-se através de campanhas de difamação, assédio online e físico, e ameaças directas à integridade e segurança dos Defensores, não apenas visando intimidá-los, mas também desencorajar e deslegitimar suas acções. Vale ressaltar que durante o processo de contagem de votos das eleições autárquicas, ocorreu uma interrupção generalizada no acesso a internet e as plataformas digitais como estratégia de obstrução ao trabalho dos DDH de observar e monitorar o processo de contagem de votos nas eleições.

Diante da aproximação das eleições e do histórico de tensões e violência que caracteriza esses períodos em Moçambique, é fundamental fortalecer a segurança digital dos DDH. Esses períodos, tradicionalmente marcados por uma intensificação da vigilância e de ataques cibernéticos, expõem os Defensores de Direitos Humanos a riscos elevados. Por isso, proteger seus dados e aparelhos eletrónicos é crucial para garantir que possam continuar a desempenhar o seu papel durante o período eleitoral. Nesse contexto, é essencial que os Defensores de Direitos Humanos estejam bem equipados para enfrentar essas ameaças, utilizando ferramentas e conhecimentos que lhes permitam navegar de forma segura no espaço digital.

Neste contexto, a RMDDH continua comprometida em dar seguimento à série de treinamentos em Segurança Digital para Defensores de Direitos Humanos em todo o país. Com estas formações e com o material comissionado a organização pretende iniciar a campanha **"Seguros, mas não Silenciosos"**, assegurando que, estes actores importantes estejam seguros enquanto continuam a expressar suas opiniões e a defender a dignidade humana.

O evento será realizado no formato virtual, no dia 18 de Setembro, das 09:00 às 12:00.

A actividade enquadra-se nos resultados do projecto PRÓ-CÍVICO E DIREITOS HUMANOS, implementado num consórcio de quatro organizações da sociedade civil, nomeadamente, Instituo para Democracia Multipartidária (IMD), Centro de Aprendizagem e Capacitação da Sociedade Civil (CESC), Fundação MASC e Centro para Democracia e Direitos Humanos (CDD).

1. **OBJECTIVO**

Com o treinamento e o material comissionado pretende-se reforçar as capacidades dos Defensores de Direitos Humanos na defesa e salvaguarda dos direitos humanos em tempo de eleições, dotando-os de conhecimentos e de competências necessárias para navegarem em segurança nas plataformas digitais durante as eleições.

1. **PERFIL DO CONSULTOR**

O candidato deve possuir qualificações académicas e/ou experiência profissional comprovadas na área de segurança digital e produção de conteúdos.

1. **ESCOPO DO TRABALHO**

O consultor tem a prerrogativa de apresentar uma proposta técnica detalhando a forma e estrutura que vai orientar a formação e os materiais para a campanha. Entretanto, a estrutura apresentada deverá contemplar os seguintes conteúdos:

|  |  |
| --- | --- |
| **CAMPANHA DE SEGURANÇA DIGITAL: SEGUROS, MAS NÃO SILENCIOSOS** | **COMO RECONHECER AMEAÇAS COMUNS**1. Como funciona a Internet;
2. Ataques de phishing;
3. Ransomware;
4. Vírus.
 |
| **COMO REFORÇAR A CONFIDENCIALIDADE**1. Criar senhas fortes (Únicas, Aleatórias e Longas);
2. Activação da autenticação multifactor e outros processos de log-In seguros;
3. Uso de gerenciadores de senhas;
4. Uso de uma VPN;
5. Configuração e utilização de e-mail seguro (criptografia PGP).
 |
| **COMO MELHORAR A PROTECÇÃO DOS DISPOSITIVOS E A SEGURANÇA DOS DADOS** 1. Uso de antivírus (pago e gratuito);
2. Actualização de sistemas operativos e programas;
3. Backup de dados importantes;
4. Configurar e usar o VeraCrypt para protecção de dados.
 |

O módulo deve ser acompanhado pelos respectivos formulários de monitoria e avaliação para permitir medir a evolução dos conhecimentos dos participantes antes e depois do treinamento e, assim, o impacto e eficácia do treinamento.

1. **PRODUTOS ESPERADOS**
* Um relatório narrativo da formação, com um máximo de 5 páginas;
* Formulários de Monitoria e Avaliação (antes e depois do treinamento);
* 20 cartazes para a campanha;
* 10 vídeos curtos para a campanha.
1. **PRAZOS**

O prazo máximo para a conclusão deste trabalho é de 10 dias úteis, contados a partir da assinatura do contrato. É imprescindível que o Consultor cumpra os prazos estabelecidos, a menos que surjam circunstâncias imprevistas que impossibilitem o cumprimento.

Caso ocorra algum evento inesperado, o Consultor poderá propor prazos alternativos e, nesse caso, serão realizadas as devidas revisões contratuais para reflectir os novos prazos acordados.

**VIII. CRONOGRAMA DE PAGAMENTOS**

* 40% após a conclusão do treinamento e entrega dos respectivos formulários de monitoria e avaliação;
* 60% após a conclusão e aprovação do material da campanha.
1. **CANDIDATURA**

Os profissionais interessados em se candidatar à posição de consultor em segurança digital são convidados a enviar suas candidaturas, até ao dia 13 de Setembro, para o endereço indicado abaixo, anexando os documentos mencionados a seguir:

* Proposta técnica delineando a metodologia proposta para alcançar os objectivos da atribuição;
* A proposta financeira detalhada em Meticais (MZN) e o equivalente em Dólares Americanos (USD);
* Curriculum Vitae.

As candidaturas devem ser enviadas para o seguinte endereço eletrónico: concursos@redemoz-defensoresdireitoshumanos.org .

Eventuais dúvidas podem ser esclarecidas pelo contacto: +258 21 085 797.

**A RMDDH reserva-se o direito de contactar apenas as propostas pré-seleccionadas.**



**Financiado por:** 

