República de Moçambique
Ministério das Comunicações e Transformação Digital

Exortação de Sua Excelência o Ministro das Comunicações e Transformação Digital por Ocasião da Celebração do Mês de Internet Mais Segura

Caros compatriotas,
Distintos representantes das instituições públicas e privadas,
Estimados parceiros, jovens e membros da sociedade civil,
Minhas senhoras e meus senhores,

É com elevada honra e profundo sentido de responsabilidade que me dirijo a todos nesta ocasião solene que assinala a celebração do Mês da Internet Mais Segura, um momento de particular relevância para o reforço do compromisso de Moçambique com a segurança digital e com a protecção dos direitos dos cidadãos, com especial atenção às nossas crianças e jovens.

A acelerada evolução tecnológica e o processo crescente de digitalização da economia, da administração pública e da vida social têm proporcionado benefícios significativos ao cidadão e ao desenvolvimento do país, promovendo maior eficiência, inclusão, inovação e acesso a serviços essenciais. Contudo, estes avanços trazem consigo novos riscos e desafios no espaço digital, que exigem uma abordagem estratégica, coordenada e responsável à **segurança cibernética**, de modo a garantir que o progresso tecnológico ocorra de forma segura, confiável e sustentável, salvaguardando os direitos dos cidadãos, a continuidade dos serviços e os interesses estratégicos do Estado.

O Governo de Moçambique, consciente dos profundos impactos da transformação digital no desenvolvimento económico, social e institucional do país, aprovou a Política de Segurança Cibernética e Estratégia da sua Implementação (PENSC), através da Resolução n.º 69/2021, de 31 de Dezembro, como instrumento orientador fundamental para a protecção do cidadão, a salvaguarda dos activos de informação, a defesa das infra-estruturas críticas e o reforço da soberania nacional no espaço cibernético.

A PENSC estabelece uma visão estratégica de longo prazo para a construção de um ecossistema digital seguro, resiliente, inclusivo e confiável, reconhecendo a segurança cibernética como um pilar essencial da boa governação, da estabilidade institucional, da confiança no uso das tecnologias digitais e da sustentabilidade do desenvolvimento nacional.

No âmbito da sua implementação, foram definidas 25 iniciativas estratégicas, que traduzem o compromisso do Estado com uma abordagem integrada e multissectorial à segurança cibernética. Entre estas iniciativas, assume particular destaque a promoção de programas estruturados de consciencialização e educação do cidadão, com especial enfoque em crianças e jovens, por se tratar da camada da população mais exposta aos riscos, abusos e práticas nocivas no ambiente digital.

O segundo dia, da segunda semana do mês de Fevereiro é reconhecido internacionalmente como o Dia da Internet Mais Segura, que, no ano de 2026, será celebrado em Moçambique no dia 10 de Fevereiro, sob o lema "**Juntos Por uma Internet Mais Segura**". Este lema recorda-nos que a segurança no espaço cibernético não é uma responsabilidade exclusiva do Governo ou das instituições, mas um dever partilhado por todos os actores da sociedade.

A celebração deste ano coloca especial enfoque a Protecção da criança e de outros grupos vulneráveis; Prevenção e combate à desinformação e à propagação de notícias falsas nas plataformas digitais, prevenção de fraudes electrónicas e burlas online, a promoção da privacidade e da protecção de dados pessoais, o reforço da literacia digital e da cultura de segurança cibernética para professores e ao cidadão bem como na promoção e defesa dos direitos humanos no ambiente digital.

Estas acções visam responder aos desafios crescentes associados ao uso intensivo da Internet e das plataformas digitais, incluindo discursos de ódio, abuso sexual online, phishing, malware e outras práticas ilícitas que comprometem a confiança, a segurança e a coesão social. Neste contexto, exortamos as escolas, instituições públicas e privadas, a sociedade civil, a academia e os meios de comunicação social para a realização de actividades de **Cidadania Digital**, reforçando a adopção de comportamentos seguros, éticos e responsáveis no espaço cibernético. Trata-se de uma efeméride de referência no calendário internacional da segurança cibernética, cuja celebração se estende ao longo de todo o mês de Fevereiro.

No actual contexto digital, a proliferação de *fake news* (desinformação) constitui uma séria ameaça à coesão social, à estabilidade institucional e à segurança dos cidadãos, na medida em que fomenta a manipulação da opinião pública, a disseminação de discursos de ódio, a prática de fraudes e a descredibilização das instituições, comprometendo a confiança no espaço público digital.

Exortamos, por isso, os cidadãos, os meios de comunicação social, os criadores de conteúdos digitais, influenciadores digitais e todas as instituições públicas e privadas a adoptarem uma postura ética, crítica e responsável no uso das plataformas digitais, verificando a credibilidade das fontes, combatendo activamente a desinformação e contribuindo para a construção de um ambiente digital seguro, confiável e promotor da verdade, do diálogo e da coesão social.

Minhas senhoras e meus senhores,

Desde a aprovação da Política Nacional de Segurança Cibernética e da respectiva Estratégia de Implementação (PENSC), o Governo de Moçambique tem registado avanços significativos e consistentes na construção de um ecossistema nacional de segurança cibernética mais robusto, coordenado e resiliente, reflectindo o compromisso do Estado com a protecção do cidadão, da economia digital e da soberania nacional no ciberespaço.

Entre os principais progressos alcançados no período de 2021-2025, destaca-se a criação e operacionalização do CSIRT Nacional, sob coordenação do INTIC, IP, que passou a desempenhar um papel central na prevenção, detecção, resposta e recuperação de incidentes de segurança cibernética, bem como na coordenação técnica a nível nacional e internacional.

Registam-se igualmente avanços relevantes na constituição da Rede Nacional de CSIRTs, que neste momento possui 12 (doze) CSIRTs, integrando equipas de resposta a incidentes ao nível do Governo, de instituições reguladoras, do sector financeiro, da academia e de algumas províncias, encontrando-se em curso a sua expansão para outros sectores estratégicos e níveis territoriais, em cumprimento das orientações da PENSC.

No domínio do quadro legal e regulatório, foram desenvolvidas e submetidas e apreciadas positivamente pelo Governo a propostas de Lei de Segurança Cibernética, a Lei de Crimes Cibernéticos, bem como o Regulamento de Centros de Dados e Regulamento de Computação em Nuvem e esta em curso a elaboração da proposta de Lei de Protecção de Dados, destacando a assinatura por Moçambique em Hanói da Convenção das Nações Unidas contra os Crimes Cibernéticos, criando as bases para um ambiente digital seguro, previsível e alinhado com boas práticas internacionais.

Ao nível da gestão de riscos e protecção das infra-estruturas críticas, foi realizado o primeiro Exercício Nacional de Avaliação de Risco Cibernético, permitindo identificar vulnerabilidades, priorizar sectores críticos e orientar a definição de medidas de mitigação baseadas em evidência.

No eixo do desenvolvimento de capacidades e consciencialização, o país tem investido fortemente na formação de quadros técnicos, decisores e outros actores-chave, bem como na realização de campanhas nacionais de sensibilização, com especial enfoque em crianças, jovens e grupos vulneráveis, em alinhamento com uma das 25 iniciativas prioritárias da PENSC.

Destaca-se, igualmente, o reforço da cooperação regional e internacional, através da participação activa de Moçambique em fóruns multilaterais, parcerias técnicas e

instrumentos internacionais de cooperação em matéria de segurança cibernética, consolidando a sua integração no ecossistema global de resposta às ameaças cibernéticas.

Estes avanços demonstram que Moçambique se encontra num percurso sólido de consolidação da sua governação da segurança cibernética, embora persistam desafios que exigem continuidade, coordenação interinstitucional e investimento sustentável para garantir a plena implementação da Política e da Estratégia nos próximos ciclos.

Minhas senhoras e meus senhores,

A Segurança Cibernética afirma-se hoje como uma prioridade estratégica global, na qual o papel dos reguladores sectoriais é determinante para assegurar a confiança, a continuidade e a resiliência dos serviços essenciais à vida económica e social. A crescente dependência dos sistemas digitais e a sofisticação das ameaças cibernéticas colocam desafios sérios à soberania, à estabilidade e ao desenvolvimento sustentável das nações.

Neste contexto, assume particular relevância o papel dos reguladores sectoriais, que têm a responsabilidade de criar e assegurar um ambiente regulatório seguro, harmonizado e resiliente, através da definição de normas, directrizes e requisitos mínimos de segurança cibernética aplicáveis aos operadores sob sua jurisdição, bem como da supervisão do cumprimento da legislação e das políticas nacionais de segurança cibernética, incluindo a Política Nacional de Segurança Cibernética e a respectiva Estratégia de Implementação.

Exortamos, por isso, os reguladores sectoriais a reforçarem o cumprimento e a implementação das orientações definidas na Política Nacional de Segurança Cibernética e na respectiva Estratégia de Implementação, incluindo a promoção e o estabelecimento de CSIRTs Sectoriais nos sectores sob sua jurisdição, assegurando a definição, aplicação e fiscalização efectiva de normas e requisitos mínimos de segurança cibernética, em prol da protecção dos cidadãos, da continuidade dos serviços essenciais e do reforço da resiliência nacional no espaço cibernético.

De igual modo, os operadores de infra-estruturas críticas e de serviços essenciais, designadamente nos sectores bancário e financeiro, das telecomunicações, da saúde, da educação, da energia, da água e do gás, assumem um papel central na salvaguarda da estabilidade e do funcionamento do país. Compete-lhes assegurar a protecção dos sistemas, dos dados e dos serviços sob sua responsabilidade, garantindo a sua disponibilidade, integridade e confidencialidade, bem como prevenir e mitigar riscos como fraudes electrónicas, ataques a sistemas de pagamento, roubo de identidade, interrupções de serviços, e outros incidentes susceptíveis de afectar a vida dos cidadãos e a economia nacional.

É igualmente sua responsabilidade proteger redes de comunicações, sistemas hospitalares, plataformas de ensino digital, dados sensíveis de cidadãos e sistemas industriais de controlo, assegurando a continuidade dos serviços essenciais, a confiança dos utilizadores e a segurança pública.

Exortamos, por isso, os operadores de infra-estruturas críticas e de serviços essenciais a reforçarem a implementação das medidas de segurança cibernética previstas na Política Nacional de Segurança Cibernética e na respectiva Estratégia de Implementação, incluindo a adopção de mecanismos robustos de gestão de riscos, a criação ou integração em CSIRTs sectoriais, a notificação atempada de incidentes ao CSIRT Nacional e o investimento contínuo em capacidades técnicas e humanas, como contributo decisivo para a resiliência nacional e a protecção do interesse público no espaço cibernético.

As entidades do sector público e privado, incluindo os municípios, encontram-se no centro do processo de transformação digital, assumindo um papel determinante na modernização dos serviços, no aumento da eficiência operacional e na promoção da inovação e da inclusão digital. Contudo, esta crescente digitalização expõe as organizações a novos riscos cibernéticos, com impacto directo na continuidade dos serviços, na protecção dos dados, na confiança dos utilizadores e na estabilidade das operações.

Exortamos, por isso, as entidades do sector público e privado a alinharem os seus processos, sistemas e práticas às orientações definidas na Política Nacional de Segurança Cibernética e na respectiva Estratégia de Implementação, reforçando a gestão de riscos digitais e adoptando medidas técnicas e organizacionais adequadas. Em particular, apelamos ao estabelecimento de CSIRTs institucionais e a sua integração em estruturas sectoriais existentes, como mecanismo essencial para a prevenção, detecção, resposta e recuperação de incidentes de segurança cibernética, bem como para a articulação efectiva com o CSIRT Nacional, contribuindo assim para o reforço da resiliência organizacional e nacional no espaço cibernético.

A academia desempenha um papel estratégico fundamental na edificação da segurança e resiliência cibernética nacional, enquanto espaço privilegiado para a formação de especialistas, a produção de conhecimento científico, a investigação aplicada e o desenvolvimento de soluções tecnológicas inovadoras que respondam aos desafios do Estado, da economia e da sociedade na Era Digital.

Exortamos, por isso, as Instituições de Ensino Superior a procederem à revisão e actualização dos seus currículos académicos, integrando de forma estruturada a segurança cibernética, a protecção de dados, a ciberdefesa, a gestão de riscos digitais e a cidadania digital, com vista à formação de quadros altamente qualificados.

Apelamos, igualmente, ao reforço da pesquisa científica e do desenvolvimento de soluções tecnológicas inovadoras, promovendo uma actuação articulada e próxima com o sector produtivo e empresarial, de modo a assegurar a transferência de conhecimento, a inovação aplicada e a criação de soluções nacionais que reduzam a dependência tecnológica externa, reforcem a soberania digital e contribuam para o crescimento económico, a competitividade e a resiliência do país no contexto digital global.

Minhas senhoras e meus senhores,

A segurança cibernética é uma responsabilidade colectiva e transversal a todos os sectores da sociedade. Cada cidadão desempenha um papel determinante na adopção de boas práticas de segurança digital, devendo manter-se informado, atento e vigilante face a ameaças como ataques de phishing, malware, violações de privacidade, desinformação, incitação ao ódio e abusos no ambiente online, particularmente aqueles que afectam crianças e jovens.

Para terminar, convido a todos os moçambicanos a unirem esforços e a assumirem um compromisso activo para garantir que a Internet seja um espaço seguro, inclusivo e promotor de oportunidades, aprendizagem e crescimento sustentável para as gerações presentes e futuras.

"Juntos Por uma Internet Mais Segura".

Muito obrigado.

Américo Muchanga

Ministro das Comunicações e Transformação Digital