Quarta-feira, 3 de Dezembro de 2025 I Série – N.º 227

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 1.360,00

SUMÁRIO

Presidente da República

PRESIDENTE DA REPÚBLICA

Decreto Presidencial n.º 256/25
de 3 de Dezembro

Considerando que a Estratégia Nacional de Cibersegurança é o documento que, dentre outras matérias, define as acções estratégicas do Estado Angolano em matéria de segurança cibernética, de acordo com as directrizes definidas pelo Executivo;

Atendendo que a implementação de uma Estratégia Nacional de Cibersegurança permitirá maximizar a resiliência do Estado Angolano na defesa do ciberespaço, promover a inovação tecnológica, gerar e garantir recursos para o País;

O Presidente da República decreta, nos termos da alínea b) do artigo 120.º e do n.º 1 do artigo 125.º, ambos da Constituição da República de Angola, o seguinte:

ARTIGO 1.º
(Aprovação)

É aprovada a Estratégia Nacional de Cibersegurança, anexa ao presente Decreto Presidencial, de que é parte integrante.

ARTIGO 2.º
(Dúvidas e omissões)

As dúvidas e omissões resultantes da aplicação e interpretação do presente Diploma são resolvidas pelo Presidente da República.

ARTIGO 3.º
(Entrada em vigor)

O presente Decreto Presidencial entra em vigor na data da sua publicação.

Apreciado em Conselho de Ministros, em Luanda, aos 27 de Outubro de 2025.

Publique-se.

Luanda, aos 26 de Novembro de 2025.

O Presidente da República, JOÃO MANUEL GONÇALVES LOURENÇO.

ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA

I. INTRODUÇÃO

Desde 2011, Angola dispõe de uma Lei de Protecção de Dados Pessoais, aprovada pela Lei n.º 22/11, de 17 de Junho. Complementando este quadro normativo, foi promulgada a Lei n.º 7/17, de 16 de Fevereiro, de Protecção das Redes e Sistemas Informáticos, Diploma que visa prevenir e combater acções que ameaçam a cibersegurança, assegurando assim a integridade da soberania territorial, com especial atenção para a protecção do ciberespaço nacional.

O referido pacote legislativo é reforçado por convenções e tratados internacionais, incorporados no ordenamento jurídico angolano. Um exemplo notável é a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, ratificada por via da Resolução n.º 33/19, de 9 de Julho, que estabelece padrões regionais para o fortalecimento da cibersegurança e protecção de dados.

Contudo, na actual era de transição digital, onde os governos enfrentam o desafio de formular políticas institucionais, legais e de gestão de recursos humanos voltadas à garantia da cibersegurança, à defesa do ciberespaço, tem sido conduzida, em grande medida, por meio de políticas de curto e médio prazos. Isso ocorre porque essas políticas, pela sua flexibilidade, podem ser ajustadas mais rapidamente que a legislação, cujo processo de alteração é intrinsecamente burocrático e frequentemente incapaz de responder à urgência das ameaças cibernéticas.

Nesse contexto, destaca-se a necessidade de aprovar uma Estratégia Nacional de Cibersegurança, instrumento essencial para estruturar políticas voltadas à prevenção e combate de práticas que comprometem o ecossistema do ciberespaço nacional. Esta Estratégia visa proteger instituições públicas e privadas, bem como indivíduos e bens, contra ciberataques, em consonância com os compromissos regionais e internacionais assumidos por Angola.

O Livro Branco das Tecnologias de Informação e Comunicação, aprovado através do Decreto Presidencial n.º 272/24, de 5 de Dezembro, que traça as medidas de política e as acções estratégicas que visam o desenvolvimento sustentável do Sector das Tecnologias de Informação e da Comunicação, enfatiza, dentre outros aspectos, a necessidade de se garantir a cibersegurança em Angola e, em particular, das suas infra-estruturas críticas e assenta em seis eixos de acção, dentre os quais se destaca o da Regulação e o da Cibersegurança.

No Domínio Político e Institucional, para além da criação e institucionalização de um Conselho Nacional de Cibersegurança, o Livro Branco das Tecnologias de Informação e Comunicação prevê a aprovação de uma Estratégia Nacional de Cibersegurança, que defina o enquadramento, os objectivos estratégicos e respectivas acções estratégicas de Angola em matéria de cibersegurança.

Nos termos, o Executivo Angolano assumiu o compromisso de adoptar medidas para a institucionalização da Estratégia Nacional de Cibersegurança, tendo como base o entendimento que a identificação dos perigos é o primeiro passo para defesa do ciberespaço, considerando que os referidos perigos são um desafio considerável para os países, principalmente membros da SADC, visto que estes apresentam défice nos mecanismos de investigação da cibercriminalidade.

No âmbito do Livro Branco das Tecnologias de Informação e Comunicação, no que a Estratégia Nacional de Cibersegurança diz respeito, o Executivo pretende alcançar três objectivos estratégicos, desdobrados conforme abaixo se apresenta:

1. Maximizar a resiliência do País no combate à cibercriminalidade;
2. Promover a inovação tecnológica;

3. Gerar e garantir recursos para o Estado.

Apesar dos esforços institucionais, políticos e legais que foram empreendidos neste domínio, o Índice Global de Cibersegurança, produzido pela União Internacional de Telecomunicações (UIT) de 2024, agência especializada das Nações Unidas em matéria de tecnologias de informação e comunicação, coloca Angola na quarta posição, a seguir ao nível mais baixo, com 39,5 pontos numa escala de 100, tendo em conta, dentre outros aspectos, a capacidade de respostas rápidas aos incidentes informáticos e a inexistência de uma estratégia nacional para este Sector.

De facto, a análise da agência assenta nas medidas legais, técnicas e organizacionais aprovadas no domínio da segurança cibernética, bem como o nível de desenvolvimento das capacidades do País no Sector e a cooperação internacional.

Para melhorar a posição supracitada no Índice Global de Cibersegurança e a avaliação do País em outros indicadores de cibersegurança, garantir a integridade das infra-estruturas críticas e a cibersegurança no geral e, desta forma, atrair investimento público e privado, sobretudo estrangeiro, o actual Executivo entende que é indispensável, dentre outras medidas, assegurar a aprovação de uma Estratégia Nacional de Cibersegurança, que se apresente como um importante documento orientador da governação cibernética.

Na verdade, dentre as várias metas prioritárias que o Executivo se propõe no quinquénio 2022-2027, destaca-se a criação da capacidade do Estado no domínio da cibersegurança, que assentará: (i) na implementação de um plano operacional de cibersegurança e dotá-lo dos meios orçamentais indispensáveis à sua implementação; (ii) na estruturação das unidades operacionais de cibersegurança, capacitando os efectivos das mesmas; e (iii) na melhoria do suporte tecnológico, adequando-o aos desafios e ameaças que enfrentamos.

II. VISÃO

Ser uma Nação segura e resiliente do ponto de vista cibernético, onde a preocupação com a segurança do espaço nacional digital é o mote da garantia dos valores mais estruturantes do Estado Democrático de Direito consagrado na Constituição da República de Angola, sem prejuízo da necessidade de preservação dos dados pessoais dos cidadãos.

III. MISSÃO

Criar e desenvolver uma capacidade legal, institucional e operacional que garanta um ambiente seguro e atrativo no ciberespaço nacional, garantindo um espaço cibernético seguro, que fomenta uma cultura de cibersegurança responsável entre os cidadãos e as instituições públicas e privadas.

IV. PRINCÍPIOS

A presente Estratégia Nacional de Cibersegurança assenta, dentre outros princípios, nos seguintes:

a) Princípio da Subsidiariedade — assenta no facto de que a responsabilidade do Estado Angolano em matéria de cibersegurança é subsidiária, uma vez que, em primeiro lugar, são os cidadãos que são chamados pela forma responsável como utilizam o

ciberespaço, em seguida, são as entidades privadas que detêm grande parte das infra-estruturas tecnológicas e, por último, o Estado que deve assegurar a integridade da Soberania Nacional, do Estado Democrático de Direito, assim como o normal funcionamento das instituições;

b) Princípio da Complementaridade — assenta na lógica de que, sendo a responsabilidade do Estado subsidiária no domínio da cibersegurança, a integridade do ciberespaço nacional constitui uma responsabilidade partilhada de todos os actores públicos, privados e cidadãos, que são os últimos beneficiários dos serviços tecnológicos;

c) Princípio da Proporcionalidade — tendo em conta que a cibersegurança decorre de um exercício complexo e continuado de avaliação dos riscos associados ao ciberespaço, este princípio implica que os recursos dispostos para mitigar os riscos identificados devem ser proporcionais aos mesmos;

d) Princípio da Inclusão e Acesso Universal — assegura que todos os cidadãos tenham acesso e podem utilizar o ciberespaço de forma segura e inclusiva;

e) Princípio da Educação e Literacia Digital — implica a promoção de ciberespaço seguro, através da implementação de programas educativos que desenvolvam competências nos cidadãos para uma participação segura, responsável e esclarecida no ciberespaço;

f) Princípio da Responsabilidade — visa a responsabilização civil e criminal pelas acções e omissões que violem direitos e interesses legalmente tutelados.

V. OBJECTIVOS GERAIS

No domínio da cibersegurança, constituem objectivos fundamentais de Angola os previstos na Constituição da República de Angola e na Lei de Segurança Nacional, nomeadamente:

a) A independência e soberania nacionais;

b) A defesa e a integridade territorial;

c) O respeito dos direitos fundamentais;

d) A segurança das populações e dos seus bens;

e) A defesa e protecção das instituições e do património nacional;

f) A manutenção da paz e da ordem pública, em condições que correspondam ao interesse nacional e estabilidade;

g) A protecção do ambiente, a biossegurança, a promoção do desenvolvimento económico e social sustentável;

h) A protecção do ciberespaço.

VI. DEFINIÇÕES

Sem prejuízo do disposto na Lei da Cibersegurança e na Lei da Segurança Nacional, para efeitos da presente Estratégia Nacional de Cibersegurança, entende-se por:

a) Ciberespaço — ambiente digital resultante da interconexão de redes de comunicação, sistemas de informação e infra-estruturas tecnológicas, incluindo a internet, redes privadas e infra-estruturas críticas, no qual ocorrem a criação, armazenamento, processamento e transmissão de dados e informações;

b) Cibersegurança — conjunto de medidas, tecnologias, políticas e práticas destinadas à protecção de redes, sistemas informáticos, infra-estruturas digitais e dados contra ameaças e ataques cibernéticos, acesso não autorizado e falhas operacionais, garantindo a confidencialidade, integridade e disponibilidade das informações no ambiente digital;

c) Ciberdefesa — a actividade que visa assegurar a defesa nacional no, ou através do ciberespaço;

d) Cibercrime — qualquer infracção penal praticada no ambiente digital ou por meio de sistemas de informação e comunicação, abrangendo tanto crimes que afectam directamente redes, dispositivos e dados, quanto aquelas facilidades pelo uso da tecnologia;

e) Ciberataque — qualquer acção maliciosa realizada por meio de redes, sistemas de informação ou dispositivos digitais, com o objectivo de comprometer a confidencialidade, integridade ou disponibilidade de dados, serviços e infra-estruturas, podendo incluir espionagem, sabotagem, roubo de informações, extorsão ou interrupção de serviços;

f) Cultura de Cibersegurança — criação e alinhamento de medidas com os objectivos da organização em estabelecer um ambiente holístico de confiança e obtenção de resultados consistentes. O que envolve a avaliação contínua do risco para a garantia de um sistema cibernético resiliente.

VII. OBJECTIVOS ESTRATÉGICOS

7.1. Objectivo Estratégico I: fortalecer as estruturas de cibersegurança

A cibersegurança é uma componente de segurança garantida, dentre outros mecanismos, por intermédio de organismos especializados habilitados para fiscalizar as acções preventivas susceptíveis de constituir ciberataques, assim como responsabilizar, se necessário, os agentes prevaricadores. É neste quadro que os Estados têm procedido com a institucionalização de Conselho Nacional de Cibersegurança, Centro Nacional de Cibersegurança e das equipas de resposta a incidentes e emergências informáticas.

É assim que, enquanto parte do «ecossistema mundial da cibersegurança», no que a garantia da integridade do ciberespaço nacional diz respeito, o Estado Angolano define como objectivo estratégico o de fortalecer as estruturas de cibersegurança.

Com o presente objectivo estratégico, procura-se dotar o País de entidades especializadas que, ao se juntar com as que já existem, possam assegurar a integridade da soberania nacional digital, fortalecer o Estado Democrático de Direito e, deste modo, garantir o normal funcionamento das instituições públicas e privadas, sem olvidar da necessidade de respeitar os direitos, liberdades e garantias individuais, por via de um sistema eficiente de protecção de dados pessoais.

7.1.1. Acções Estratégicas

Para assegurar o fortalecimento das estruturas de cibersegurança, são definidas as seguintes acções estratégicas:

a) Reforçar a capacidade das instituições nacionais no domínio de defesa cibernética, com vista a maximizar a resiliência das forças de defesa e segurança para fazer face a incidentes, ciberameaças ou efectivos ciberataques que periguem os interesses nacionais e a soberania digital;

b) Criar o Conselho Nacional de Cibersegurança — concebido como órgão de natureza consultiva do Titular do Poder Executivo em matéria de cibersegurança, que será um passo crucial para fortalecer o País neste domínio, sendo composto por todos os organismos públicos e privados que lidam com o ciberespaço e cibersegurança, designadamente representantes de outros Departamentos Ministeriais e demais entidades públicas, bem como representantes da sociedade civil e entidades privadas com actuação no domínio da cibersegurança;

c) Criar o Centro Nacional de Cibersegurança — que será concebido como uma entidade pública que integra a Administração Indirecta do Estado, ficando sob o poder de superintendência do Titular do Poder Executivo, podendo ser delegado ao Titular do Departamento Ministerial responsável pelas Telecomunicações, Tecnologias de Informação e Comunicação Social — MINTTICS;

d) Institucionalizar as equipas de resposta à emergência informática, assim como as equipas de resposta a incidentes de segurança informática, CERT.ao e CSIRTs, cujo funcionamento estará integrado organicamente no Centro Nacional de Cibersegurança;

e) Promover uma maior articulação e coordenação das entidades supracitadas que operarão em matéria de cibersegurança em Angola, através da criação de sinergias com entidades públicas que integram o Sistema de Segurança Nacional e com entidades privadas que intervêm no ecossistema cibernético;

f) Reforçar as capacidades da Procuradoria-Geral da República e, em particular, do Serviço de Investigação Criminal, robustecendo as suas estruturas e as suas capacidades humanas e técnicas para a investigação e combate ao cibercrime, fomentando os recursos humanos alocados a estas entidades e a sua capacidade de executar medidas de obtenção de provas com recursos aos mais avançados meios tecnológicos, assim como a resposta às exigências de cooperação internacional em matéria de cibersegurança;

g) Reforçar o papel das comunidades das equipas de respostas a incidentes e emergências de cibersegurança como plataforma de excelência para a resposta operacional coordenada e a partilha de boas práticas e de informação relativa a incidentes;

h) Aprofundar a coordenação e cooperação entre as diversas entidades nacionais com responsabilidades na cibersegurança, tendo em vista uma melhor capacidade de alerta e resposta a incidentes e emergências cibernéticas.

7.2. Objectivo Estratégico II: criar a consciência e estimular a cultura e literacia em cibersegurança

Conforme resulta do Livro Branco das Tecnologias de Informação e Comunicação, a literacia em cibersegurança é uma temática que tem ganho cada vez mais ênfase na sociedade e a procura de informação sobre este assunto tem crescido exponencialmente. Assim, no actual contexto, os utilizadores de internet e dos dispositivos de conexão a ela podem ter comportamentos diferenciados no seu uso.

Na maioria das vezes, os referidos comportamentos podem não ser os mais seguros e correctos, resultando em consequências que impactam negativamente as suas vidas, como, por exemplo, observar os seus dispositivos electrónicos, sendo alvo de um ataque cibernético. Daí, ser necessário a criação de políticas que visam elevar a literacia em matéria de cibersegurança, visando o uso correcto da internet e dos dispositivos de conexão a este importante meio de comunicação digital, sobretudo em crianças.

No contexto digital em que se encontra o Mundo, onde o ciberespaço tornou-se um dos motes do desenvolvimento socioeconómico e político de cada País, do mesmo modo em que cresce o risco para as empresas, cidadãos e instituições públicas e privadas, faz-se necessário que, para além de entender os riscos decorrentes do uso inapropriado das redes e sistemas informáticos, a sociedade e os cidadãos se antecipem e estejam preparados para enfrentar os problemas que daí surgirem.

A antecipação supracitada passa primordialmente pela consciencialização e partilha de informação, permitindo uma avaliação antecipada e eficaz das ameaças emergentes da utilização do ciberespaço, visando a detecção das ciberameaças e ciberataques antes que os danos se manifestem. Com efeito, é indispensável que os cidadãos desenvolvam uma compreensão clara das ameaças que o uso inadequado das tecnologias de informação e comunicação apresenta.

É neste contexto que o Executivo Angolano pretende promover acções de consciencialização, sensibilização e de capacitação dos cidadãos, em particular de crianças e jovens, para que estes adoptem comportamentos positivos na utilização segura dos serviços digitais. Estas acções permitirão abordar temáticas de Cidadania e Literacia Digital, bem como os riscos associados à navegação online e modo de comunicação entre os utilizadores das plataformas de tecnologias de informação e comunicação, promovendo a confiança e segurança dos utilizadores no reforço da utilização da internet.

7.2.1. Acções Estratégicas

Para assegurar a criação da consciência e cultura de cibersegurança, pretende-se reforçar a consciencialização e a educação neste domínio por via das seguintes acções estratégicas:

a) Incentivar os órgãos públicos e empresas privadas para que realizem campanhas de conscientização internas;

b) Realizar acções de conscientização da população:

i. Criar políticas públicas que promovam a conscientização da sociedade sobre cibersegurança;

c) Promover a consciência e literacia digital, através de programas educativos de sensibilização. Com este objectivo, pretende-se capacitar os cidadãos com competências que lhes permitam avaliar e discernir qualquer conteúdo publicado na internet. Trata-se de habilitar os cidadãos por via de fornecimento de competências necessárias para nave-

gar com confiança, consciência e segurança. A concretização deste objectivo passará, fundamentalmente, pela criação de uma série de iniciativas específicas centradas nas acções de capacitação, educação e consciencialização da população em geral;

d) Promover a confiança e segurança dos cidadãos em serviços *online*, na certeza de que tenham a necessária confiança nestes serviços, através de mecanismos que permitam avaliar o grau de percepção de segurança nas redes e sistemas informáticos, assegurando que os serviços digitais sejam seguros;

e) Fomentar a pesquisa e o desenvolvimento em cibersegurança;

f) Criar programas de capacitação continuada para profissionais do Sector Público e do Sector Privado;

g) Capacitar os cidadãos para o uso da internet e das plataformas de acesso de forma positiva, informada e segura, mediante iniciativas de alfabetização, massificação, inclusão digital e o reforço das tecnologias de informação e comunicação no sistema de ensino;

h) Promover a literacia digital infanto-juvenil, através de: (i) promoção da Segurança na Internet, isto é, ensinar sobre a importância da privacidade e segurança *online*; (ii) disseminação de conceitos básicos sobre a introdução à programação, no sentido de ensinar a lógica de programação; (iii) desenvolvimento de parcerias com as academias do ensino infanto-juvenil; (iv) introdução de conceitos básicos de robótica; (v) divulgação ampla de conceitos sobre realidade virtual e aumentada e como elas podem ser usadas em diferentes áreas; (vi) explicação dos conceitos básicos de inteligência artificial, como aprendizado de máquina, redes neurais e algoritmos de inteligência artificial. Para promover a literacia digital infanto-juvenil, principalmente no ensino primário, dentre outras acções, com base nestas directrizes serão tomadas as seguintes acções estratégicas:

Incluir a tecnologia como parte do currículo escolar — para o acesso às Telecomunicações/TIC e aprendizagem de como usá-la adequadamente desde cedo. As escolas podem oferecer aulas que ensinam habilidades básicas de computação e acesso à internet;

Enfatizar a segurança *online* — de modo a aprenderem sobre os riscos da internet, incluindo privacidade, *bullying online* e fraude. É importante que os professores discutam esses assuntos com seus alunos e ensinem boas práticas de segurança *online*;

Incentivar a criatividade — de modo que sejam encorajadas a usar de forma atractiva as tecnologias e criando conteúdos, quer praticando jogos educativos ou usando a internet para pesquisar sobre assuntos interessantes;

Ensinar habilidades de pesquisa — por forma a aprender como usar os mecanismos de busca de forma efectiva e como avaliar a qualidade das informações encontradas na internet.

7.3. Objectivo Estratégico III: desenvolver e fortalecer as capacidades nacionais de cibersegurança

No presente século, a informação e o conhecimento exercem um papel fundamental no crescimento e reforço da competitividade dos países, especialmente nos que estão em vias de desenvolvimento, impondo que os sistemas de educação e formação profissional impactem positivamente no desenvolvimento socioeconómico e no equilíbrio social e cultural. Neste sentido, a aposta num modelo de ensino orientado para as tecnologias de informação e comunicação, reforçando os conteúdos e disciplinas neste domínio ao nível do ensino básico, secundário e universitário, permitindo que a população e os jovens em particular se familiarizem com matérias de cibersegurança, desde muito cedo.

Com efeito, tendo em conta que a criação da consciência e da cultura de cibersegurança não é suficiente para municiar os cidadãos e instituições com capacidades para prevenir ciberataques e cibercrimes, pretende-se, ainda, desenvolver e fortalecer as capacidades do País e, principalmente, dos cidadãos em matéria de cibersegurança.

Neste sentido, pretende-se dedicar maior atenção no investimento na formação especializada e na educação dos jovens a partir do ensino de base para que estes percebam, desde muito cedo, como se deve correctamente utilizar os serviços digitais, em articulação com outros sectores, isto passará pela criação de cursos, programas e disciplinas de cibersegurança, com ênfase na protecção das infra-estruturas críticas, ao nível das escolas e das instituições do ensino superior públicas e privadas.

Com este objectivo estratégico pretende-se, do ponto de vista específico, promover a formação, educação e capacitação profissional em cibersegurança, através da criação de cursos, programas educativos, disciplinas e outras acções de educação técnico-profissional nas escolas secundárias e no ensino superior. Pretende-se, no fundo, promover a realização de acções de formação e de capacitação profissional nos sectores público e privado, bem como na sociedade civil, em matéria de segurança cibernética.

O desenvolvimento e o fortalecimento das capacidades nacionais de cibersegurança assentarão, ainda, na aplicação das tecnologias de informação e comunicação na educação, que deverá contribuir: (i) na melhoria da eficiência da gestão do sistema de ensino e escolar; (ii) na melhoria do preparo dos estudantes para o mercado de trabalho; (iii) na facilitação do acesso aos conteúdos e profissionais de qualidade, em especial em locais de baixa densidade demográfica ou difícil acesso; e (iv) na oferta de melhores oportunidades a estudantes com limitações físicas, tais como limitações de visão, audição ou locomoção.

7.3.1. Acções Estratégicas

Para o desenvolvimento e o fortalecimento das capacidades nacionais de cibersegurança são definidas as seguintes acções estratégicas:

a) Promover uma cultura digital em toda a população, através da criação de um quadro nacional de competências digitais e de desenvolvimento, de competências digitais na população em geral com especial atenção aos diferentes grupos vulneráveis;

b) Promover a produção científica, o desenvolvimento e a inovação nos vários domínios da segurança cibernética;

c) Desenvolver competências digitais em alunos e professores do sistema de educação, bem como promover a formação especializada de profissionais e técnicos de telecomunicações de informação e comunicação;

d) Propor a inclusão da cibersegurança por intermédio de suas competências básicas e do uso ético da informação na educação básica, educação infantil, ensino fundamental e ensino médio;

e) Estimular a criação de cursos de nível superior em cibersegurança;

f) Incentivar a formação de profissionais para actuar no combate aos crimes cibernéticos;

g) Incorporar tecnologias digitais na política educacional e formação técnico-profissional;

h) Actualizar programas de formação em tecnologias digitais de acordo com as necessidades actuais e futuras do mercado;

i) Promover a educação em ciência, tecnologia, engenharia, artes e matemática em meninas, meninos e adolescentes, com especial atenção para as tecnologias emergentes;

j) Fortalecer o uso de ambientes virtuais em suas diferentes modalidades;

k) Promover a criação, adopção e disseminação de recursos educacionais digitais aberta entre todos os intervenientes no sistema educativo nacional;

l) Incorporar tecnologias digitais para transformar a gestão do ciclo de vida educacional;

m) Promover a certificação técnica especializada em tecnologias digitais;

n) Promover uma cultura de estudos avançados e pesquisas em tecnologias digital da academia e centros de pesquisa;

o) Promover a realização de eventos de formação de curta duração, como *hackathons* e actividades de treinamento focadas na aprendizagem por projectos;

p) Introduzir a tecnologia de forma gradual e adaptada à idade dos alunos, para que comece com actividades simples, como a utilização de computadores e *tablets* para pesquisar informações sobre assuntos escolares;

q) Ensinar aos alunos como utilizar a internet de forma segura, incluindo informações simples sobre senhas fortes, privacidade *online* e segurança ao compartilhar informações pessoais;

r) Incentivar os alunos a participar de actividades criativas, como a criação de animações ou jogos simples, utilizando ferramentas digitais;

s) Utilizar jogos educativos para ensinar matérias importantes, como matemática e ciência;

t) Ensinar aos alunos sobre a importância do respeito e da empatia no ambiente *online*, incluindo a importância de evitar o *cyberbullying* e de tratar os outros com respeito e tolerância;

u) Incentivar os alunos a utilizar a tecnologia para colaborar com outros alunos em projectos escolares, promovendo o trabalho em equipa e a resolução de problemas.

7.4. Objectivo Estratégico IV: consolidar a legislação nacional de cibersegurança

Reconhecendo a importância da legislação na garantia da integridade do ciberespaço nacional e na repressão de cibercrimes, o País dispõe, dentre outros instrumentos normativos nacional e de âmbito internacional vigente no ordenamento jurídico interno, de uma Lei de Protecção das Redes e Sistemas Informáticos, bem como de uma Lei de Protecção de Dados Pessoais.

No entanto, a Lei de Protecção das Redes e Sistemas Informáticos necessita de ser adaptada ao actual contexto nacional e internacional de cibersegurança, de modo a tornar o País um lugar seguro em matéria de cibersegurança, sem se preocupar com eventuais ciberataques. Com efeito, há o reconhecimento de que, face à dinâmica do Sector das Tecnologias de Informação e Comunicação, a legislação existente carece de permanente actualização e é necessário legislar sobre novas áreas que emergem dos desafios específicos relativos às novas tecnologias, como as *fake news*, OTTs, inteligência artificial e a regulamentação da propriedade intelectual das obras produzidas com recurso à IA.

Em articulação com o Livro Branco das Tecnologias de Informação e Comunicação, o processo de reforma legislativa obedecerá duas fases, nomeadamente a fase 1 — que consiste na aprovação das leis que conformam a reforma legislativa, por parte do poder legislativo, e da legislação estruturante que regulamenta o novo quadro normativo, pelo Poder Executivo; a fase 2 — correspondente à regulamentação da legislação complementar por parte dos poderes delegados aos Departamentos Ministeriais.

7.4.1. Acções Estratégicas

Para a consolidação da legislação nacional em matéria de cibersegurança são definidas as seguintes acções estratégicas:

a) Rever e harmonizar o quadro jurídico-legal existente. Neste domínio, pretende-se alterar a Lei de Protecção de Redes e Sistemas Informáticos de modo a adequá-la à capacidade de resposta do País em matéria de cibersegurança e aos desafios que o ciberespaço internacional impõe;

b) Reforçar o quadro jurídico-legal sobre a cibersegurança em Angola;

c) Ratificar convenções internacionais sobre cibersegurança que ainda não estejam em vigor no ordenamento jurídico angolano;

d) Assinar acordos de cooperação judiciária em matérias de criminalidade cibernética;

e) Assinar tratados internacionais sobre cibersegurança;

f) Avaliar, no âmbito da cibercriminalidade, a necessidade de ajustamento das normas processuais penais aos desafios globais que se colocam e a eventual cooperação com operadores de comunicações estrangeiros e a agilização de acções de investigação *online*;

g) Promover e divulgar o quadro jurídico-legal sobre cibersegurança;

h) Harmonizar a estrutura departamental que caracteriza o Sector das Telecomunicações e Tecnologias de Informação com os objectivos estratégicos do Executivo no domínio das tecnologias de informação e comunicação, promovendo a transição para uma sociedade mais inclusiva do ponto de vista da utilização dos serviços digitais.

7.5. Objectivo Estratégico V: adoptar e implementar boas práticas de cibersegurança

Para além de reforçar a defesa das infra-estruturas digitais contra ciberameaças, a adopção e implementação de medidas legais, políticas e institucionais que visam garantir a integridade do ciberespaço instaura a confiança entre cidadãos, empresas e parceiros internacionais, o que é fundamental para a atracção de investimento estrangeiro, diversificação da economia nacional e a solidificação da presença de Angola no panorama internacional no que a cibersegurança diz respeito.

7.5.1. Acções Estratégicas

No domínio da adopção e implementação de boas práticas internacionais de cibersegurança, são definidas as seguintes acções estratégicas:

a) Promover a aplicação os recomendáveis padrões internacionais de cibersegurança ao nível do sector público e privado;

b) Adoptar padrões internacionais de cibersegurança nos sectores público e privado, bem como a implementação rigorosa de critérios de cibersegurança nos processos de aquisição de *software* e *hardware*;

c) Reforçar a resposta aos riscos de cibersegurança, incluindo o uso da criptografia para proteger dados em trânsito e em repouso, garantindo a privacidade e integridade das informações;

d) Incentivar o crescimento da indústria de cibersegurança, promovendo serviços de consultoria especializados e avaliações de risco para a terceirização de serviços de tecnologias de informação e comunicação;

e) Elaborar e aprovar novos instrumentos normativos sobre tecnologias emergentes.

7.6. Objectivo Estratégico VI: cooperar no âmbito internacional

No contexto actual, em que os países e povos se encontram interligados e interdependentes através da internet e do uso dos serviços digitais, aos Estados incumbe não apenas a defesa da soberania do seu espaço digital como, também, garantir a segurança e defesa do ciberespaço internacional; facto que demanda uma eficiente cooperação e colaboração entre os países.

É neste quadro que a presente Estratégia enfatiza a necessidade do Estado Angolano em geral e das entidades que directamente lidam com cibersegurança, em particular, cooperar com outros Estados e organizações regionais e internacionais em busca de melhores soluções dos problemas actuais de cibersegurança.

7.6.1. Acções Estratégicas

No Domínio da Cooperação Internacional, são definidas as seguintes acções estratégias:

a) Contribuir para a regulação e universalização do ciberespaço internacional, promovendo o respeito do direito internacional aplicável, a patilha transparente da sua governação entre todos os actores, a respectiva acessibilidade universal e a disseminação de boas práticas de utilização;

b) Aprofundar a participação de Angola nas organizações e eventos regionais e internacionais no domínio de cibersegurança;

c) Participar no exercício aprofundado da cibersegurança, reforçando e aumentando o nível de maturidade para a protecção do ciberespaço internacional, onde a partilha da informação seja um factor-chave;

d) Integrar organismos regionais e internacionais de cibersegurança, com vista à participação, cooperação internacional e afirmação de Angola em matéria de cibersegurança;

e) Desenvolver, no âmbito da actuação internacional, a ciberdiplomacia como a disciplina da acção externa do Estado que visa promover, dentre outras matérias, a aplicação do direito internacional vigente ao ciberespaço, a fim de garantir a respectiva estabilidade, a governação transparente e partilhada da sua utilização universal e a criação eficiente de capacidades normativas;

f) Desenvolver o quadro internacional da ciberdiplomacia em que Angola venha a se inserir, identificando iniciativas prioritárias das organizações internacionais, regionais ou intergovernamentais de intercâmbio de boas práticas a que deverá aderir.

VIII. AVALIAÇÃO, MONITORIZAÇÃO E REVISÃO DA ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA

A presente Estratégia Nacional de Cibersegurança será objecto de avaliação anual, submetida a aprovação do Titular do Poder Executivo, após a sua apreciação pelo Conselho Nacional de Cibersegurança, sob proposta do Departamento Ministerial responsável pelo Sector das Telecomunicações e Tecnologias de Informação.

A avaliação anual visa assegurar a verificação do cumprimento dos Objectivos Estratégicos, do Plano de Acção e da adequação dos mesmos na proporção da evolução das circunstâncias, nos termos da Lei e no Estatuto Orgânico do Conselho Nacional de Cibersegurança.

É da competência do Secretariado Executivo do Conselho Nacional de Cibersegurança a monitorização da presente Estratégia Nacional de Cibersegurança, conforme previsto na Lei e no Estatuto Orgânico que o rege.

Por outro lado, a Estratégia será objecto de revisão quinquenal, sem prejuízo da revisão extraordinária, na medida em que as circunstâncias cibernéticas assim o exijam.

O Presidente da República, João Manuel Gonçalves Lourenço.

(25-0487-B-PR)

PRESIDENTE DA REPÚBLICA

Decreto Presidencial n.º 257/25
de 3 de Dezembro

Considerando que as Instituições de Ensino Superior ministram cursos de graduação e de pós-graduação e, consequentemente, atribuem graus e títulos académicos;

Havendo a necessidade de se estabelecer as regras e os procedimentos para a atribuição de graus e títulos académicos outorgados pelas Instituições de Ensino Superior;

Atendendo ao disposto no n.º 3 do artigo 13.º e o n.º 6 do artigo 108.º, ambos da Lei n.º 17/16, de 7 de Outubro, alterada pela Lei n.º 32/20, de 12 de Agosto;

O Presidente da República decreta, nos termos da alínea m) do artigo 120.º e do n.º 4 do artigo 125.º, ambos da Constituição da República de Angola, o seguinte:

ARTIGO 1.º
(Aprovação)

É aprovado o Regulamento de Atribuição de Graus e Títulos Académicos conferidos no Subsistema de Ensino Superior, anexo ao presente Decreto Presidencial, de que é parte integrante.

ARTIGO 2.º
(Dúvidas e omissões)

As dúvidas e omissões suscitadas na interpretação e aplicação do presente Diploma são resolvidas pelo Presidente da República.

ARTIGO 3.º
(Entrada em vigor)

O presente Decreto Presidencial entra em vigor na data da sua publicação.

Apreciado em Conselho de Ministros, em Luanda, aos 27 de Outubro de 2025.

Publique-se.

Luanda, aos 3 de Dezembro de 2025.

O Presidente da República, JOÃO MANUEL GONÇALVES LOURENÇO.