BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.

AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República».**

SUMÁRIO

ASSEMBLEIA DA REPÚBLICA

Lei n.º 13/2026

de 1 de Julho

Havendo necessidade de estabelecer o regime jurídico da Segurança Cibernética que visa responder de forma eficaz e eficiente aos desafios da Sociedade da Informação, bem como garantir a segurança do Estado, das instituições, do cidadão, e a protecção de sistemas de informação e Infra-estruturas Críticas no espaço cibernético, ao abrigo do disposto no número 1, do artigo 178 da Constituição da República, a Assembleia da República determina:

CAPÍTULO I

Disposições Gerais

ARTIGO 1

(Objecto)

A presente Lei estabelece o regime jurídico aplicável à Segurança Cibernética, visando garantir a segurança do Estado, das instituições, do cidadão, bem como assegurar a protecção de redes de comunicação de dados, de sistemas de informação e de infra-estruturas críticas no espaço cibernético.

ARTIGO 2

(Âmbito de aplicação)

1. A presente Lei aplica-se a:
   a) Administração Pública;
   b) Sector Privado;
   c) Operador de Rede de Infra-estruturas críticas;
   d) Provedores Intermediários de Serviços;
   e) Provedores de Serviços Digitais;
   f) Operador de Rede de Serviços Essenciais;
   g) Provedores de Serviços de Segurança Cibernética;
   h) Operadores de Plataformas Digitais;
   i) Operadores de Comunicações Electrónicas;
   j) Pessoas singulares e outras entidades que utilizam redes de comunicação de dados e sistemas de informação.
2. Exceptuam-se do previsto no número 1 do presente artigo:
   a) as entidades da Administração Pública em acções sobre redes de comunicação de dados, sistemas de informação e infra-estruturas críticas para fins de defesa nacional, segurança interna e de Estado;
   b) as entidades da Administração Pública em acções sobre redes e sistemas de informação que processem informação classificada conforme a legislação aplicável.
3. Caso uma entidade se enquadre simultaneamente em mais de uma das alíneas constantes do número 1, do presente artigo, aplica-se o regime mais exigente para a segurança das redes e dos sistemas de informação.

ARTIGO 3

(Definições)

As definições dos termos e os acrónimos usados na presente Lei constam do Glossário em anexo I e II, que dela fazem parte integrante.

ARTIGO 4

(Princípios)

A presente Lei rege-se pelos seguintes princípios:

a) Colaboração e cooperação – consiste no dever das partes de colaborar, cooperar e respeitar os mecanismos de funcionamento do Sistema Nacional de Segurança Cibernética, ao nível interno e internacional, de modo a garantir a transparência e eficácia na governação da Segurança Cibernética;

b) Protecção dos direitos humanos – consiste na utilização segura das Tecnologias de Informação e Comunicação, de forma a garantir o pleno respeito pelos direitos humanos, incluindo o direito à liberdade de expressão e de privacidade;

c) Cadeia de valor – consiste na adopção de medidas que permitam a integridade com vista a que o cidadão confie na segurança dos produtos e serviços disponibilizados com recurso a Tecnologias de Informação e Comunicação;

d) Transparência - políticas e práticas de segurança cibernética devem fornecer informação claras sobre objectivos, métodos e limites das actividades não fazendo o uso de funções ocultas e prejudiciais no domínio das Tecnologias de Informação e Comunicação;

e) Divulgação de vulnerabilidades - encorajar a divulgação responsável de vulnerabilidades de segurança cibernética;

f) Responsabilidade - consiste na abstenção de produção ou uso de soluções prejudiciais ao ecossistema tecnológico;

g) Integridade - garantia de que os dados, sistemas e operações de tecnologia de informação e comunicação permaneçam precisos, completos e livres de manipulação não autorizada;

h) Legalidade - as autoridades responsáveis pela segurança cibernética devem actuar com base em competências legalmente definidas;

i) Proporcionalidade - assegura que as medidas adoptadas pelo Estado ou por entidades privadas para prevenir, detectar e responder a ameaças no espaço cibernético sejam adequadas, necessárias e equilibradas em relação aos fins que pretendem alcançar;

j) Necessidade - que orienta a legitimidade das medidas adoptadas para prevenir, detectar e responder a ameaças no espaço cibernético;

k) Privacidade - assegura que as medidas adoptadas para garantir a segurança cibernética não violam indevidamente a esfera privada dos cidadãos.

CAPÍTULO II

Organização do Sistema Nacional de Segurança Cibernética

ARTIGO 5

(Segurança Cibernética)

A Segurança Cibernética é o conjunto de políticas, conceitos de segurança, ferramentas, garantias de segurança, directrizes, abordagens de gestão de risco, acções, capacitações, boas práticas, aplicáveis para proteger o ambiente cibernético e activos das pessoas físicas e colectivas.

ARTIGO 6

(Estrutura)

O Sistema Nacional de Segurança Cibernética é composto por órgãos e entidades e obedece a seguinte estrutura:

a) Órgãos:

i. Conselho Nacional de Segurança Cibernética;

ii. Autoridade Nacional de Segurança Cibernética;

iii. Equipa Nacional de Resposta a Incidentes de Segurança Cibernética (CSIRT Nacional);

b) Entidades:

i. Rede Nacional de CSIRTs;

ii. Operadores de Infra-estruturas Críticas;

iii. Provedores Intermediários de Serviços Electrónicos;

iv. Operadores de Serviços Essenciais;

v. Provedores de Serviços Digitais;

vi. Operadores de Plataformas Digitais;

vii. Operadores de Centros de Dados;

viii. Operadores de Plataformas de Computação em Nuvem;

ix. Provedores de Serviços de Segurança Cibernética;

x. Operadores de Comunicações Digitais;

xi. Unidades especializadas em operações cibernéticas para as actividades de defesa nacional, segurança interna e segurança do Estado.

SUBSECÇÃO I

Conselho Nacional de Segurança Cibernética

ARTIGO 7

(Natureza)

O Conselho Nacional de Segurança Cibernética, abreviadamente designado por CNSC é o órgão multisectorial de coordenação e de governação específica para assuntos relativos a Segurança Cibernética e é presidido pelo Primeiro-Ministro.

ARTIGO 8

(Composição)

1. O Conselho Nacional de Segurança Cibernética tem a seguinte composição:

a) Os titulares que superintendem as seguintes áreas:

i. Defesa Nacional;

ii. Segurança Interna;

iii. Segurança de Estado;

iv. Finanças;

v. Tecnologias de Informação e Comunicação;

vi. Justiça;

vii. Transportes;

viii. Economia;

ix. Negócios Estrangeiros e Cooperação;

x. Educação;

xi. Saúde;

xii. Género, Criança e Acção social;

xiii. Energia;

xiv. Água;

xv. Mar, Águas Interiores;

xvi. Pescas;

xvii. Juventude;

xviii. Administração Pública.

b) Representantes das seguintes entidades:

i. Regulador de TIC;

ii. Regulador das Comunicações;

iii. Regulador do Sector Financeiro;

iv. Regulador do Sector de Águas;

v. Regulador do Sector de Energia;

vi. Regulador do Sector de Investigação Científica em Saúde Humana;

vii. Procuradoria Geral da República;

viii. Serviço Nacional de Investigação Criminal;

ix. Equipa Nacional de Resposta a Incidentes de Segurança Cibernética (CSIRT Nacional);

x. Embaixador Itinerante para a área de TIC;

xi. Centro de Coordenação Cibernética das Forças de Defesa e Segurança (CCCFDS).

2. Sempre que se mostre necessário, desde que devidamente fundamentada a pertinência, podem ser convidadas outras entidades, para matérias específicas.

3. Os representantes do sector empresarial, da academia e da sociedade civil são designados pelas respectivas organizações.

ARTIGO 9

(Competências)

Compete ao Conselho Nacional de Segurança Cibernética:

a) assegurar a coordenação político-estratégica para a segurança do espaço cibernético;

b) monitorar a implementação da Estratégia Nacional de Segurança Cibernética;

c) pronunciar-se sobre a Estratégia Nacional de Segurança Cibernética;

d) elaborar anualmente, ou sempre que necessário, relatório de avaliação da implementação da Estratégia Nacional de Segurança Cibernética;

e) propor ao Governo a aprovação de decisões de carácter programático relacionadas com a definição e implementação da Estratégia Nacional de Segurança Cibernética;

f) emitir parecer sobre matérias relativas à segurança cibernética;

g) responder às solicitações por parte do Governo, no âmbito das suas competências.

SUBSECÇÃO II

Autoridade Nacional de Segurança Cibernética

ARTIGO 10

(Natureza)

A Autoridade Reguladora de Tecnologias de Informação e Comunicação é a Autoridade Nacional de Segurança Cibernética no âmbito da presente Lei.

ARTIGO 11

(Competências)

Compete à Autoridade Nacional de Segurança Cibernética:

a) garantir a coordenação técnica para a segurança do espaço cibernético;

b) regular, supervisionar, fiscalizar e aplicar sanções no âmbito da segurança cibernética;

c) garantir que o País use o espaço cibernético de uma forma livre, confiável e segura, através da promoção da melhoria contínua da segurança cibernética nacional e da cooperação internacional, em articulação com as autoridades competentes;

d) registar e licenciar os Provedores de Serviços de Segurança Cibernética;

e) auditar as Entidades do Sistema Nacional de Segurança Cibernética e outros sectores;

f) credenciar estabelecimentos de prestação de serviços de segurança cibernética, incluindo laboratórios de investigação forense digital estabelecidos para investigar crimes cibernéticos e mitigar incidentes de segurança cibernética;

g) credenciar profissionais de segurança cibernética;

h) emitir orientações ou avisos aos prestadores de serviços, intermediários, centros de dados, pessoas jurídicas e qualquer outra pessoa com o objectivo de melhorar a segurança cibernética da infra-estrutura de informação do País;

i) definir e implementar medidas e instrumentos necessários à antecipação, detecção, reacção e recuperação de situações que, face à iminência e ocorrência de incidentes cibernéticos ponham em causa o interesse nacional;

j) garantir a protecção de Infra-estruturas Críticas em coordenação com as entidades reguladoras sectoriais competentes;

k) propor ao Governo a actualização da lista de serviços essenciais;

l) servir de ponto de contacto único nacional para efeitos de cooperação internacional, sem prejuízo das atribuições legais das Forças de Defesa e Segurança e da autoridade que superintende a área de investigação criminal relativas à cooperação internacional em matéria específica;

m) definir o nível nacional de alerta e emitir instruções de segurança cibernética;

n) estabelecer códigos de conduta, padrões e normas na área de segurança cibernética alinhados com as boas práticas nacionais e internacionais;

o) actuar como órgão central do Sistema Nacional de Segurança Cibernética;

p) proteger a soberania e os interesses nacionais no espaço cibernético;

q) alertar ao Governo sobre as principais ameaças no espaço cibernético.

ARTIGO 12

(Estado de sítio ou de emergência)

1. Em caso de estado de sítio ou de emergência, as funções da Autoridade Nacional de Segurança Cibernética são exercidas pelo Centro de Coordenação Cibernética das Forças de Defesa e Segurança, nas seguintes situações:

a) agressão efectiva ou eminente;

b) grave ameaça;

c) perturbação da ordem constitucional.

2. Sempre que se julgar necessário o Centro de Coordenação Cibernética das Forças de Defesa e Segurança articula com a Entidade Reguladora de Tecnologias de Informação e Comunicação para melhor cumprimento das funções de Segurança Cibernética no País.

SUBSECÇÃO III

Equipa Nacional de Resposta a Incidentes de Segurança Cibernética

ARTIGO 13

(Natureza)

1. A Equipa Nacional de Resposta a Incidentes de Segurança Cibernética, abreviadamente designada por nCSIRT.MZ, é o órgão de coordenação operacional e estratégica para prevenir e responder aos incidentes de segurança cibernética em articulação com as Equipas de Resposta a Incidentes de Segurança Cibernética Sectoriais e Institucionais existentes.

2. A nCSIRT.MZ funciona na Entidade Reguladora de Tecnologias de Informação e Comunicação.

ARTIGO 14

(Competências)

Compete à Equipa Nacional de Resposta a Incidentes de Segurança Cibernética:

a) coordenar as acções de resposta a incidentes de segurança e ser o ponto central de notificações a nível nacional e internacional;

b) recolher, analisar e divulgar a informação sobre vulnerabilidades e alertas de incidentes de segurança cibernética com vista a prevenir e mitigar os crimes cibernéticos em Moçambique;

c) avaliar vulnerabilidades e realizar testes de penetração da infra-estrutura em rede de organizações governamentais e das infra-estruturas críticas;

d) estabelecer as medidas técnicas e operacionais de resposta aos ataques, roubos, furtos e quaisquer outros incidentes cibernéticos;

e) coordenar a Rede Nacional de CSIRTs;

f) servir de elo de ligação entre as redes nacionais de CSIRTs e a Autoridade Nacional de Segurança Cibernética;

g) supervisionar as equipas sectoriais e institucionais de resposta a incidentes de Segurança Cibernética com particular incidência nos sectores das infra-estruturas críticas de informação;

h) promover a adopção e a utilização de normas técnicas e práticas padronizadas;

i) operacionalizar acções que visam estudos de pesquisa e análise de tráfego da *Internet;*

j) monitorar, colectar, analisar o tráfego da *Internet* e elaborar estatísticas;

k) consciencializar a sociedade em matérias de segurança cibernética.

SUBSECÇÃO IV

Entidades do Sistema Nacional de Segurança Cibernética

ARTIGO 15

(Rede Nacional de CSIRTs)

1. A Rede Nacional de CSIRTs é um *fórum* para a troca de informação sobre incidentes cibernéticos entre o CSIRT Nacional, os CSIRTs sectoriais e CSIRTs institucionais.

2. A Rede Nacional de CSIRTs opera sob coordenação da Entidade Reguladora de Tecnologias de Informação e Comunicação através do CSIRT Nacional.

3. Os CSIRTs institucionais partilham informação sobre incidentes cibernéticos e sua mitigação aos CSIRTs sectoriais e CSIRT Nacional.

4. Os CSIRTs sectoriais partilham informação sobre incidentes cibernéticos e sua mitigação ao CSIRT Nacional.

SUBSECÇÃO V

Operadores de Infra-estruturas Críticas

ARTIGO 16

(Natureza)

O Operador de Infra-estrutura Crítica é uma entidade pública ou privada responsável por assegurar o funcionamento contínuo de infra-estruturas críticas.

ARTIGO 17

(Obrigações)

1. São obrigações do Operador de Infra-estrutura Crítica:

a) estabelecer o CSIRT institucional;

b) aplicar um conjunto de medidas e técnicas que proporcionam a segurança e protecção dos activos considerados essenciais para o bom funcionamento das infra-estruturas críticas;

c) adoptar uma abordagem de gestão de riscos para identificar, compreender e mitigar os riscos para prevenir incidentes cibernéticos;

d) dispor de procedimentos sólidos para recuperar o mais rápido possível de incidentes cibernéticos;

e) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;

f) fornecer comunicações de informações que tenham conteúdo criminoso ou que atenta contra segurança do Estado mediante decisão judicial ou administrativa, devidamente fundamentada;

g) aplicar medidas de gestão e processos de supervisão eficazes, incluindo planos com objectivos e responsabilização claros, bem como um processo que se adapte aos riscos identificados.

2. Para o exercício das suas actividades os Operadores de Infra-estruturas Críticas devem registar-se na Autoridade Nacional de Segurança Cibernética.

SUBSECÇÃO VI

Provedor Intermediário de Serviços Electrónicos

ARTIGO 18

(Natureza)

O Provedor Intermediário de Serviços Electrónicos é uma entidade pública ou privada que, em representação de outra pessoa, envia, recebe, ou armazena mensagens de dados, presta serviços de acesso à rede ou serviços a partir dela.

ARTIGO 19

(Obrigações)

1. São obrigações do Provedor Intermediário de Serviços Electrónicos:

a) registar os utilizadores dos seus serviços;

b) aplicar medidas necessárias para governação, identificação e protecção do risco cibernético, detecção, resposta e recuperação de ataques cibernéticos;

c) garantir o acesso e assegurar a comunicação de informação transmitida pelos utilizadores a ele vinculados, através de uma rede ou sistema de comunicação;

d) implementar medidas de segurança cibernética que cumpram com padrões e normas de segurança cibernética nas suas infra-estruturas de TIC's para proteger o sistema de segurança cibernética, estabelecidas no regime jurídico aplicável;

e) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;

f) fornecer comunicações de informações que tenham conteúdo criminoso ou que atentem contra a segurança do Estado mediante decisão judicial ou administrativa, devidamente fundamentada;

g) colaborar com as autoridades competentes sempre que se mostrar necessário.

2. Para o exercício das suas actividades o Provedor Intermediário de Serviços Electrónicos deve registar-se na Autoridade Nacional de Segurança Cibernética.

SUBSECÇÃO VII

Operador de Serviços Essenciais

ARTIGO 20

(Natureza)

1. O Operador de Serviço Essencial é uma entidade pública ou privada que presta um serviço primário para a manutenção de actividades sociais ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço.

2. A lista de entidades que actuam nos sectores e subsectores que operam serviços essenciais constam do Anexo II da presente Lei.

3. A actualização da lista dos serviços essenciais é feita pelo Conselho de Ministros.

ARTIGO 21

(Obrigações)

1. São obrigações do Operador de Serviços Essenciais:

a) estabelecer o CSIRT institucional;

b) aplicar medidas necessárias para governação, identificação e protecção do risco cibernético, detecção, resposta e recuperação de ataques cibernéticos;

c) dispor de procedimentos sólidos para recuperar o mais rápido possível de incidentes cibernéticos;

d) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;

e) fornecer à entidade competente comunicações de informações que tenham conteúdo criminoso ou que atenta contra segurança do Estado mediante decisão judicial ou administrativa, devidamente fundamentada.

2. Para o exercício das suas actividades o Operador de Serviço Essenciais deve registar-se na Autoridade Nacional de Segurança Cibernética e comunicar ao CSIRT Nacional.

SUBSECÇÃO VIII

Provedor de Serviços Digitais

ARTIGO 22

(Natureza)

O Provedor de Serviços Digitais é uma pessoa colectiva pública ou privada que presta serviços oferecidos por meio electrónicos, em que todas as informações são transmitidas e acedidas por meio de uma rede de dados.

ARTIGO 23

(Obrigações)

1. São obrigações do Provedor de Serviços Digitais:

a) registar os utilizadores dos seus serviços;

b) estabelecer o CSIRT institucional;

c) aplicar medidas necessárias para governação, identificação e protecção do risco cibernético, detecção, resposta e recuperação de ataques cibernéticos;

d) dispor de procedimentos sólidos para recuperar o mais rápido possível de incidentes cibernéticos;

e) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;

f) fornecer dados dos utilizadores quando solicitados por autoridades competentes ou colaborar com as autoridades competentes sempre que se mostrar necessário, autorizado por despacho de um Juiz de instrução criminal;

g) colaborar com as autoridades competentes sempre que se mostrar necessário.

2. Para o exercício das suas actividades o Provedor de Serviços Digitais deve registar-se na Autoridade Nacional de Segurança Cibernética.

SUBSECÇÃO IX

Operadores de Plataformas Digitais

ARTIGO 24

(Natureza)

O Operador de Plataformas Digitais é uma pessoa colectiva pública ou privada provedora de aplicações da *Internet* que explora profissionalmente e com fins económicos as plataformas digitais.

ARTIGO 25

(Obrigações)

1. São obrigações do Operador de Plataformas Digitais:

a) registar os utilizadores das suas plataformas;

b) estabelecer o CSIRT institucional;

c) aplicar medidas necessárias para governação, identificação e protecção do risco cibernético, detecção, resposta e recuperação de ataques cibernéticos;

d) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;

e) fornecer dados dos utilizadores quando solicitados por autoridades competentes ou colaborar com as autoridades competentes sempre que se mostrar necessário, autorizado por despacho de um Juiz de instrução criminal;

f) colaborar com as autoridades competentes sempre que se mostrar necessário.

2. Para o exercício das suas actividades o Operador de Plataformas Digitais deve registar-se na Autoridade Nacional de Segurança Cibernética.

3. O Operador de Plataformas Digitais que presta serviços ao Estado está sujeito à regulamentação específica.

SUBSECÇÃO X

Operador de Centros de Dados

ARTIGO 26

(Natureza)

O Operador de Centro de Dados é uma entidade pública ou privada que presta serviços de armazenamento, tratamento e transmissão de dados, que engloba estruturas ou grupos de estruturas destinadas ao alojamento, à interligação e à operação centralizada de equipamento de redes de comunicação de dados e tecnologias de informação.

ARTIGO 27

(Obrigações)

1. São obrigações do Operador de Centros de Dados:

a) registar os seus utilizadores;

b) estabelecer o CSIRT institucional;

c) garantir que os dados conservados sejam da mesma qualidade e sujeitos a mesma protecção e segurança dos dados em trânsito na rede;

d) adoptar medidas técnicas e organizacionais adequadas à protecção de dados contra destruição, perda, alteração ou divulgação não autorizada;

e) adoptar medidas para evitar os incidentes cibernéticos que afectam a segurança das suas redes e sistemas de informação e para reduzir ao mínimo o seu impacto nos serviços digitais, a fim de assegurar a continuidade desses serviços;

f) fornecer dados dos utilizadores quando solicitados por autoridades competentes ou colaborar com as autoridades competentes sempre que se mostrar necessário, autorizado por despacho de um Juiz de instrução criminal;

g) colaborar com as autoridades competentes sempre que se mostrar necessário.

2. Para o exercício das suas actividades o Operador de Centros de Dados deve registar-se na Autoridade Nacional de Segurança Cibernética.

3. O Operador de Centros de Dados que presta serviços ao Estado está sujeito à regulamentação específica.

SUBSECÇÃO XI

Operador de Plataformas de Computação em Nuvem

ARTIGO 28

(Natureza)

O Operador de Plataformas de Computação em Nuvem é uma pessoa singular, colectiva pública ou privada que forneça directa ou indirectamente um conjunto de recursos flexíveis, escaláveis físicos ou virtuais compartilháveis.

ARTIGO 29

(Obrigações)

1. São obrigações do Operador de Plataformas de Computação em Nuvem, as seguintes:

a) estabelecer o CSIRT institucional;

b) registar os seus utilizadores;

c) garantir que os dados conservados sejam da mesma qualidade e sujeitos a mesma protecção e segurança dos dados em trânsito na rede;

d) adoptar medidas técnicas e organizacionais adequadas à protecção de dados contra destruição, perda, alteração ou divulgação não autorizada;

e) adoptar medidas técnicas e organizacionais necessárias à antecipação, detecção, reacção e recuperação dos danos causados por incidentes cibernéticos.

2. Para o exercício das suas actividades o Operador das Plataformas de Computação em Nuvem, deve registar-se na Autoridade Nacional de Segurança Cibernética.

3. O Operador de Serviço de Computação em Nuvem Privada que presta serviços ao Estado está sujeito a regulamentação específica.

SUBSECÇÃO XII

Provedor de Serviços de Segurança Cibernética

ARTIGO 30

(Natureza)

O Provedor de Serviço de Segurança Cibernética é uma pessoa singular, colectiva pública ou privada licenciada para prestar serviços de segurança cibernética, relacionados com tratamento de incidentes, gestão de vulnerabilidades, teste de penetração, serviços forenses digitais, governação de segurança cibernética, gestão do risco, conformidade, formação e outros serviços de segurança cibernética.

ARTIGO 31

(Obrigações)

1. São obrigações do Provedor de Serviços de Segurança Cibernética:

a) descrever os serviços oferecidos e os processos técnicos envolvidos;

b) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;

c) adoptar medidas técnicas e organizacionais necessárias à antecipação, detecção, reacção e recuperação dos danos causados por incidentes cibernéticos;

d) adoptar uma abordagem de gestão de riscos para identificar, compreender e mitigar os riscos para prevenir incidentes cibernéticos.

2. Para o exercício das suas actividades o Provedor de Segurança Cibernética deve registar-se na Autoridade Nacional de Segurança Cibernética e comunicar ao CSIRT Nacional o exercício da sua actividade.

SUBSECÇÃO XIII

Operador de Comunicações Digitais

ARTIGO 32

(Natureza)

Operador de Comunicações Digitais é uma entidade pública ou privada que fornece um serviço que permite que vários utilizadores enviem mensagens ou documentos para uma variedade de outras pessoas ou interajam em tempo real por meio de voz e vídeo.

ARTIGO 33

(Obrigações)

1. São obrigações do Operador de Comunicações Digitais:

a) registar os seus utilizadores;

b) estabelecer o CSIRT institucional;

c) garantir que os dados conservados sejam da mesma qualidade e sujeitos a mesma protecção e segurança que os dados na rede;

d) adoptar medidas técnicas e organizacionais adequadas à protecção de dados contra destruição, perda, alteração ou divulgação não autorizada;

e) descrever os serviços oferecidos e os processos técnicos envolvidos;

f) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados.

2. Para o exercício das suas actividades o Operador de Comunicações Digitais deve registar-se na Autoridade Nacional de Segurança Cibernética.

CAPÍTULO III

Segurança das Redes e dos Sistemas de Informação

SECÇÃO I

Segurança de Redes

ARTIGO 34

(Segurança de Redes de Comunicação de Dados)

Cabe as Entidades e aos operadores de plataformas de comunicação de dados assegurar a integridade, a confidencialidade e a privacidade das comunicações mediante a implementação de medidas de segurança lógica e física, estabelecidas no regime jurídico aplicável.

ARTIGO 35

(Protecção do Sistema de Nomes de Domínio)

Compete a Entidade Reguladora de Tecnologias de Informação e Comunicação, garantir a segurança do Sistema de Nomes de Domínio (DNS) através de utilização de ferramentas específicas, evitando ataques do DNS e fraudes na *Internet,* nos termos a regulamentar.

ARTIGO 36

(Resposta a Incidentes no Espaço Cibernético)

1. Os Reguladores sectoriais e os Governos Provinciais devem estabelecer CSIRTs sectoriais, provinciais e garantir a criação de CSIRTs institucionais.

2. Os sectores com infra-estruturas críticas e as demais instituições dos sectores públicos, privado, academia e sociedade civil, incluindo municípios devem estabelecer CSIRTs institucionais.

3. Os membros da Rede Nacional de CSIRTs devem estabelecer confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança.

4. Os membros da Rede Nacional de CSIRTs devem colaborar para criar os mecanismos necessários à prevenção e à resposta rápida num cenário de incidente de segurança cibernética.

ARTIGO 37

(Segurança de dados de tráfego)

1. Os processadores e controladores de dados específicos armazenados numa rede de comunicações electrónicas e sistemas da sociedade da informação, incluindo os dados de tráfego, devem assegurar a sua confidencialidade, segurança e ordenar a conservação expedita dos dados.

2. Os dados referidos no número 1 do presente artigo devem ser preservados por um período mínimo de 1 ano.

ARTIGO 38

(Armazenamento não explícito de dados de tráfego e de localização)

Os Provedores Intermediários de Serviços no Espaço Cibernético ou os Provedores de Serviços Digitais, a quem o armazenamento de dados de tráfego e de localização, relativos à uma determinada comunicação de dados que tenha sido ordenada à conservação devem indicar as outras entidades que nela participam, permitindo a identificação das mesmas, nos termos a regulamentar.

ARTIGO 39

(Acesso ao Sistema de Informação e Preservação de Provas)

1. Os Provedores Intermediários de Serviços no Espaço Cibernético e os Provedores de Serviços Digitais que tenham armazenado num determinado Sistema de Informação, dados de tráfego e de localização necessários à produção de provas, tendo em vista a descoberta da verdade, deve disponibilizar o controlo desses dados ou permitir o acesso ao Sistema de Informação onde os mesmos estejam armazenados, sempre que solicitado pelas autoridades competentes, nos termos da lei.

2. Os dados referidos no número 1 do presente artigo devem ser conservados por um período de 1 ano, contados a partir da data da conclusão da comunicação.

3. O período de preservação de provas definido no número 2 do presente artigo pode ser prorrogado nos casos justificados mediante decisão judicial.

ARTIGO 40

(Preservação de dados)

1. Os Provedores Intermediários de Serviços acessíveis ao público e os Prestadores de Armazenagem Principal devem conservar os dados de tráfego e de localização, bem como os dados conexos, para identificar o assinante ou o utilizador de um serviço digital acessível ao público ou de um serviço de armazenagem principal, quando tais dados sejam por si gerados ou tratados no território nacional e no âmbito da sua actividade, exclusivamente para fins de investigação, detenção e repressão de crimes.

2. Os dados referidos no número 1 do presente artigo devem ser conservados num período de 1 ano, contados a partir da data da conclusão da comunicação.

3. O período de preservação de dados definido no número anterior pode ser prorrogado nos casos justificados mediante decisão judicial.

ARTIGO 41

(Identificação e localização do endereço do Protocolo de *Internet*)

As entidades definidas na presente Lei devem conservar para o efeito de identificação e localização do endereço do Protocolo de *Internet* (IP), os seguintes dados:

a) a identificação dos endereços físicos dos equipamentos que usaram o referido endereço IP;

b) os mapas de endereçamento das redes;

c) os dados que identificam a localização geográfica do endereço IP, tomando como referência os registos das Entidades Regionais de Registos da *Internet,* responsáveis pela distribuição e gestão dos endereços IP e sistema autónomo.

ARTIGO 42

(Comunicação iniciada ou concluída no território nacional)

Os Provedores Intermediários de Serviços Acessíveis ao público devem conservar dados em que a comunicação não seja iniciada ou concluída no território nacional.

SECÇÃO II

Segurança nos Sistemas de Informação

ARTIGO 43

(Segurança nos Sistemas)

As entidades definidas na presente Lei devem garantir a segurança de qualquer dispositivo ou conjunto de dispositivos

que procedem ao armazenamento, tratamento, recuperação ou transmissão de dados informáticos em execução de um programa de computador.

ARTIGO 44

(Infra-estrutura de Tecnologias de Informação e Comunicação)

1. As entidades definidas na presente Lei devem aplicar medidas e técnicas que garantem a segurança e protecção dos activos considerados essenciais para o bom funcionamento das infra-estruturas.

2. As medidas e técnicas previstas no número 1 do presente artigo, são estabelecidas nos termos a regulamentar.

SECÇÃO III

Programas de Computador e Bases de Dados

ARTIGO 45

(Programas de computador)

As medidas e técnicas para programas de computador, são aplicáveis na presente Lei, sem prejuízo do regime jurídico das TIC's previsto na legislação em vigor.

ARTIGO 46

(Bases de dados)

A utilização das bases de dados deve obedecer às medidas e técnicas de protecção para acesso, armazenamento, duplicação de arquivos, tratamento e recuperação de informação automatizada, sem prejuízo do disposto no regime jurídico das Transacções Electrónicas.

CAPÍTULO IV

Requisitos de Segurança e Notificação de Incidentes

SECÇÃO I

Requisitos gerais de segurança

ARTIGO 47

(Requisitos de segurança)

1. A Autoridade Nacional da Segurança Cibernética deve estabelecer e actualizar requisitos de segurança cibernética de forma a permitir a utilização de padrões, normas e especificações técnicas internacionalmente aceites sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.

2. Os requisitos de segurança cibernética são definidos nos termos a regulamentar.

ARTIGO 48

(Requisitos mínimos de segurança)

1. Sem prejuízo dos requisitos de segurança definidos em regulamentação específica, os requisitos mínimos de segurança devem obedecer:

a) a política de segurança de informação;

b) a metodologia de gestão do risco cibernético;

c) os procedimentos de notificação de incidentes;

d) os mecanismos de prevenção, correcção ou mitigação do risco cibernético;

e) a infra-estrutura de cópias de segurança e reposição;

f) os mecanismos de auditoria interna de segurança e de supervisão;

g) a conformidade com a legislação e as normas aplicáveis ao sector;

h) o programa de capacitação e consciencialização permanente aos colaboradores em matérias de segurança cibernética;

i) a existência do responsável pela segurança de informação;

j) a existência de equipa de detecção e resposta a incidentes de segurança cibernética.

2. Os requisitos mínimos de segurança são de cumprimento obrigatório por todas entidades abrangidas pela presente Lei.

3. Sem prejuízo dos requisitos de segurança definidos em regulamentação específica, os requisitos mínimos de segurança devem garantir um nível adequado de protecção das redes e sistemas de informação, tendo em conta o risco identificado e os desenvolvimentos tecnológicos e devem ter em conta os seguintes factores:

a) a definição de uma Política de Segurança da Informação clara e objectiva;

b) o estabelecimento de uma metodologia de gestão do risco cibernético eficaz;

c) a criação de procedimentos rápidos para a notificação e resposta a incidentes de segurança;

d) a implementação de medidas de prevenção, correcção ou mitigação de riscos cibernéticos;

e) a manutenção de sistemas de cópias de segurança e recuperação de dados eficientes;

f) a implementação de auditorias internas e mecanismos de supervisão contínua da segurança;

g) a garantia da conformidade com a legislação e normas aplicáveis ao sector;

h) a capacitação e consciencialização dos colaboradores em matéria de segurança cibernética;

i) a nomeação de um responsável pela segurança da informação, com autoridade para garantir o cumprimento das medidas de segurança;

j) a criação de uma equipa especializada na detecção e resposta a incidentes de segurança cibernética.

4. Os requisitos mínimos de segurança são obrigatórios para todas as entidades abrangidas pela presente Lei, com o objectivo de assegurar a protecção eficaz contra ameaças cibernéticas.

ARTIGO 49

(Sujeição a requisitos de segurança e de notificação de incidentes)

1. Constituem entidades sujeitas aos requisitos de notificação de incidentes as seguintes:

a) Administração Pública e Sector Privado;

b) Operadores de Infra-estruturas Críticas;

c) Provedores Intermediários de Serviços no Espaço Cibernético;

d) Operadores de Serviços Essenciais;

e) Provedores de Serviços Digitais;

f) Operadores de Centros de Dados;

g) Operadores de Plataformas de Computação em Nuvem;

h) quaisquer outras entidades que utilizam redes e sistemas de informação.

2. Os requisitos de notificação de incidentes são definidos nos termos previstos em regulamentação específica.

ARTIGO 50

(Requisitos de Segurança para a Administração Pública e Sector Privado)

1. As entidades da Administração Pública e do Sector Privado devem tomar as medidas técnicas e organizacionais adequadas previstas na presente Lei e em regulamento específico, tendo em conta os progressos técnicos mais recentes, para garantir um nível de segurança adequado ao risco em causa nas redes e sistemas de informação.

2. O responsável pela área administrativa das entidades da Administração Pública e do Sector Privado deve nomear o responsável e o auditor interno da segurança cibernética para melhor gestão de riscos cibernéticos.

3. As entidades da Administração Pública e do Sector Privado devem criar uma Política de Segurança de Informação Institucional, para proteger os dados e garantir a integridade, confidencialidade e disponibilidade das informações.

4. As entidades da Administração Pública e do Sector Privado devem estabelecer um CSIRT institucional.

5. As medidas técnicas e organizacionais são objecto de regulamentação específica.

ARTIGO 51

(Requisitos de Segurança para Operadores de Infra-estruturas Críticas)

1. Os Operadores de Infra-estruturas Críticas devem tomar as medidas técnicas e organizacionais adequadas previstas na presente Lei e em regulamento específico, tendo em conta os progressos técnicos mais recentes, para garantir um nível de segurança adequado ao risco em causa nas redes e sistemas de informação.

2. O responsável pela área administrativa dos Operadores de Infra-estruturas Críticas, deve nomear o responsável e o auditor interno da segurança cibernética para melhor gestão de riscos cibernéticos.

3. Os Operadores de Infra-estruturas Críticas Privados devem estabelecer um CSIRT institucional.

ARTIGO 52

(Requisitos de Segurança para os Operadores de Serviços Essenciais)

1. Os Operadores de Serviços Essenciais devem cumprir as medidas técnicas e organizacionais adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.

2. As medidas técnicas e organizacionais previstas no número 1 do presente artigo devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.

3. Os Operadores de Serviços Essenciais devem tomar as medidas adequadas para evitar os incidentes que afectam a segurança das redes e dos sistemas de informação utilizados para a prestação dos seus serviços essenciais e para reduzir o seu impacto, a fim de assegurar a continuidade desses serviços.

ARTIGO 53

(Requisitos de segurança para Provedores de Serviços Digitais)

1. Os Provedores de Serviços Digitais devem tomar as medidas técnicas e organizacionais, adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam no contexto da oferta dos serviços digitais.

2. As medidas técnicas referidas no número 1 do presente artigo, devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes e devem ter em conta os seguintes factores:

a) a segurança dos sistemas, infra-estruturas e das instalações;

b) o tratamento dos incidentes;

c) a gestão da continuidade das actividades;

d) o acompanhamento, a auditoria e os testes realizados;

e) a conformidade com as normas internacionais.

3. Os Provedores de Serviços Digitais devem tomar medidas para prevenir incidentes que afectam a segurança das suas redes e sistemas de informação.

ARTIGO 54

(Requisitos de segurança para os Provedores Intermediários de Serviços Digitais)

1. Os Provedores Intermediários de Serviços Digitais devem identificar e tomar as medidas técnicas e organizacionais, adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam no contexto da oferta dos serviços digitais.

2. As medidas técnicas, organizacionais referidas no número 1 do presente artigo, devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, obedecendo os progressos técnicos mais recentes, tendo em conta os seguintes factores:

a) segurança dos sistemas, Infra-estruturas Críticas e das instalações;

b) tratamento dos incidentes;

c) gestão da continuidade das actividades;

d) acompanhamento, a auditoria e os testes realizados;

e) conformidade com as normas internacionais.

3. Os Provedores Intermediários de Serviços Digitais devem aplicar medidas para evitar os incidentes que afectam a segurança das suas redes e sistemas de informação para assegurar a continuidade desses serviços.

4. As medidas técnicas e organizacionais referidas nos números 1, 2 e 3 do presente artigo são estabelecidas nos termos a regulamentar.

ARTIGO 55

(Requisitos de segurança para Operadores de Centros de Dados)

1. Um operador de Centro de Dados é uma entidade responsável por monitorar, gerir e manter a infra-estrutura física e lógica de uma instalação de processamento de dados.

2. O Operador de Centro de Dados deve tomar medidas adequadas para garantir a integridade, confidencialidade e a disponibilidade dos dados armazenados, reduzindo os riscos de tempo de inactividade.

ARTIGO 56

(Requisitos de segurança para Operadores de Plataformas de Computação em Nuvem)

1. Os Operadores de Plataformas de Computação em Nuvem devem garantir a segurança no armazenamento de dados na nuvem, em conformidade com as boas práticas reconhecidas internacionalmente.

2. Os requisitos de segurança são definidos nos termos da regulamentação específica.

SECÇÃO II

Notificação de Incidentes de Segurança Cibernética

ARTIGO 57

(Incidentes de segurança cibernética de impacto significativo)

1. Considera-se que um incidente de segurança cibernética tem um impacto significativo, em termos de grau de danos ou de custos para uma organização, se atender, a pelo menos, uma das seguintes condições:

a) o impacto do incidente de segurança cibernética, é classificado em menos ou mais grave, de acordo com o grau de consequências determinado na avaliação do risco realizado;

b) devido ao incidente de segurança cibernética, a prestação do serviço essencial não pode continuar depois de decorrido o tempo máximo de interrupção admissível do serviço, de acordo com o nível de serviço ou requisitos relevantes para a continuidade dos negócios ou serviço;

c) a continuidade do serviço de algum outro prestador de serviço essencial é interrompida devido ao incidente de segurança cibernético;

d) para resolver o incidente de segurança cibernética, é necessário aplicar qualquer das medidas extraordinárias estabelecidas na avaliação do risco realizado ou em outro documento, se houver, que descreva a reintegração da continuidade do serviço ou da segurança do sistema de informação;

e) os serviços oferecidos pela Infra-estrutura Crítica, ou o provedor de outro serviço ou usuários do serviço sofrem ou podem sofrer danos devido ao incidente de segurança cibernética.

2. O impacto significativo de incidentes cibernéticos é objecto de regulamentação específica.

ARTIGO 58

(Notificação de incidentes para a Administração Pública e Sector Privado)

1. As entidades devem notificar ao respectivo CSIRT Sectorial e ao CSIRT Nacional os incidentes com um impacto significativo na segurança das redes de comunicação de dados e dos sistemas de informação, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética.

2. As notificações das entidades da Administração Pública devem incluir informações que permitam ao CSIRT do Governo e ao CSIRT Nacional determinar o impacto dos incidentes.

3. A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4. A fim de determinar a relevância do impacto de um incidente deve-se ter em conta os seguintes parâmetros:

a) o número de utilizadores afectados;

b) a duração do incidente;

c) a distribuição geográfica, no que se refere à zona afectada pelo incidente.

5. A Autoridade Nacional de Segurança Cibernética deve prestar ao notificante as informações relevantes relativas ao seguimento da sua notificação.

6. A Autoridade Nacional de Segurança Cibernética, após consultar o notificante, deve divulgar incidentes específicos de acordo com o interesse público, salvaguardando a segurança e os interesses dos Operadores de Infra-estruturas Críticas.

7. As entidades da Administração Pública devem submeter ao CSIRT da Administração Pública, o CSIRT do Governo, e para o CSIRT Nacional o relatório mensal da resposta e da resolução do incidente.

8. O relatório da resposta e da resolução de incidentes inclui informações relativas às causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 59

(Notificação de incidentes para Operadores de Infra-estruturas Críticas)

1. Os Operadores de Infra-estruturas Críticas devem notificar ao respectivo CSIRT sectorial e ao CSIRT Nacional os incidentes com um impacto significativo na segurança das redes e dos sistemas de informação, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética.

2. A notificação dos Operadores de Infra-estruturas Críticas deve incluir informação que permite ao CSIRT sectorial e ao CSIRT Nacional determinar o impacto dos incidentes.

3. A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4. A fim de determinar a relevância do impacto de um incidente deve-se ter em conta, os seguintes parâmetros:

a) o número de utilizadores afectados pelo incidente, em particular os utilizadores que dependem do serviço para prestarem os seus próprios serviços;

b) a duração do incidente;

c) a distribuição geográfica, no que se refere à zona afectada pelo incidente;

d) o nível de gravidade da perturbação do funcionamento do serviço;

e) a extensão do impacto nas actividades económicas e sociais.

5. A Autoridade Nacional de Segurança Cibernética deve prestar ao notificante as informações relevantes relativas ao seguimento da sua notificação.

6. A Autoridade Nacional de Segurança Cibernética deve divulgar os incidentes específicos de acordo com o interesse público, salvaguardando a segurança e os interesses dos Operadores de Infra-estruturas Críticas.

7. Os Operadores de Infra-estruturas Críticas devem submeter ao CSIRT sectorial e ao CSIRT Nacional o relatório mensal sobre a resposta e resolução do incidente.

8. O relatório de resposta e resolução de incidentes inclui informações sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 60

(Notificação de incidentes para os Operadores de Serviços Essenciais)

1. Os Operadores de Serviços Essenciais devem notificar ao respectivo CSIRT Sectorial e ao CSIRT Nacional os incidentes com um impacto significativo na continuidade dos serviços essenciais por si prestados, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética.

2. A notificação deve incluir informação que permite à Autoridade Nacional de Segurança Cibernética determinar o impacto dos incidentes.

3. A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4. A fim de determinar a relevância do impacto de um incidente deve-se ter em conta, os seguintes parâmetros:

a) o número de utilizadores afectados pelo incidente, em particular os que dependem do serviço para prestarem os seus próprios serviços;

b) a duração do incidente;

c) a distribuição geográfica, no que se refere à zona afectada pelo incidente;

d) o nível de gravidade da perturbação do funcionamento do serviço;

e) a extensão do impacto nas actividades económicas e sociais.

5. A Autoridade Nacional de Segurança Cibernética deve:

a) informar os pontos de contacto únicos dos outros CSIRTs, caso o incidente tenha um impacto significativo na continuidade dos serviços essenciais;

b) salvaguardar a segurança e os interesses do Operador de Serviços Essenciais, bem como a confidencialidade da informação prestada na sua notificação;

c) prestar ao Operador de Serviços Essenciais as informações relevantes, relativas ao seguimento da sua notificação;

d) transmitir as notificações referidas no número 1, do presente artigo, aos pontos de contacto únicos dos outros CSIRT;

e) divulgar informação relativa a incidentes específicos de acordo com o interesse público.

6. O Operador de Serviços Essenciais que depende de um terceiro prestador de serviços para a prestação de um serviço essencial, notifica todos os impactos importantes na continuidade dos seus serviços, decorrentes dos incidentes cibernéticos.

7. Os Operadores de Serviços Essenciais submetem ao CSIRT Sectorial e ao CSIRT Nacional o relatório mensal da resposta e da resolução do incidente.

8. O relatório da resposta e da resolução de incidentes inclui informação sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 61

(Notificação de incidentes para Provedores de Serviços Digitais)

1. Os Provedores de Serviços Digitais devem notificar ao respectivo CSIRT sectorial e ao CSIRT Nacional os incidentes com um impacto significativo na continuidade dos serviços essenciais por si prestados, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética.

2. A notificação referida no número 1 do presente artigo, inclui informação que permite à Autoridade Nacional de Segurança Cibernética determinar o impacto do incidente.

3. A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4. A fim de determinar se o impacto de um incidente é substancial, são tidos em conta os seguintes parâmetros:

a) o número de utilizadores afectados pelo incidente, em particular os utilizadores que dependem do serviço para prestarem os seus próprios serviços;

b) a duração do incidente;

c) a distribuição geográfica, no que se refere à zona afectada pelo incidente;

d) o nível de gravidade da perturbação do funcionamento do serviço;

e) a extensão do impacto nas actividades económicas e sociais.

5. A Autoridade Nacional de Segurança Cibernética, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público.

6. Os Provedores de Serviços Digitais são obrigados a submeter ao CSIRT sectorial e para o CSIRT Nacional o relatório mensal da resposta e da resolução do incidente.

7. O relatório da resposta e da resolução de incidentes inclui informação sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 62

(Notificação de incidentes para os Provedores Intermediários de Serviços)

1. Os Provedores Intermediários de Serviços Digitais devem notificar a Autoridade Nacional de Segurança Cibernética dos incidentes com impacto substancial na prestação dos serviços digitais, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética.

2. A notificação referida no número 1 do presente artigo, inclui informação que permite à Autoridade Nacional de Segurança Cibernética determinar a importância dos impactos transfronteiriços.

3. A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4. A fim de determinar se o impacto de um incidente é substancial, são tidos em conta os seguintes parâmetros:

a) o número de utilizadores afectados pelo incidente, em particular os utilizadores que dependem do serviço para prestarem os seus próprios serviços;

b) a duração do incidente;

c) a distribuição geográfica, no que se refere à zona afectada pelo incidente;

d) o nível de gravidade da perturbação do funcionamento do serviço;

e) a extensão do impacto nas actividades económicas e sociais.

5. A Autoridade Nacional de Segurança Cibernética, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público.

6. Os Provedores Intermediários de Serviços Digitais são obrigados a submeter ao CSIRT sectorial e para o CSIRT Nacional o relatório mensal da resposta e da resolução do incidente.

7. O relatório da resposta e da resolução de incidentes inclui informação sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 63

(Notificação de incidentes para Operadores de Centros de Dados)

1. Os Operadores de Centros de Dados devem:

a) notificar à Autoridade Nacional de Segurança Cibernética dos incidentes com impacto substancial na prestação dos serviços, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética;

b) notificar seus assinantes atempadamente, justificando quaisquer incidentes de segurança cibernética, incluindo o vazamento de dados e o que afecta ou pode afectar o conteúdo do assinante;

c) notificar ao CSIRT Nacional atempadamente de qualquer incidente de segurança cibernética ou vazamento de dados que tenham conhecimento e o que afecta ou pode afectar o conteúdo do assinante;

d) adoptar regras e políticas internas para garantir a continuidade do negócio, recuperação de desastres e gestão de riscos, devendo fornecer aos assinantes um resumo dessas regras e políticas;

e) submeter ao CSIRT sectorial e ao CSIRT Nacional o relatório mensal da resposta e da resolução do incidente.

2. O relatório da resposta e da resolução de incidentes inclui informação sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 64

(Notificação de incidentes para Operadores de Plataformas de Computação em Nuvem)

1. Os Operadores de Plataformas de Computação em Nuvem devem:

a) notificar a Autoridade Nacional de Segurança Cibernética dos incidentes com impacto substancial na prestação dos serviços, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética nos termos regulamentares;

b) notificar aos seus assinantes atempadamente, justificando quaisquer incidentes de segurança cibernética, incluindo vazamento de dados e o que afecta ou pode afectar o conteúdo do assinante;

c) notificar ao CSIRT Nacional de imediato de qualquer incidente de segurança cibernética e vazamento de dados de que tenha conhecimento;

d) adoptar regras e políticas internas para a continuidade do negócio, recuperação de desastres, gestão de riscos e fornecer aos assinantes dos serviços um resumo dessas regras e políticas;

e) submeter ao CSIRT Sectorial e ao CSIRT Nacional o relatório mensal da resposta e da resolução do incidente.

2. O relatório de resposta e resolução de incidentes inclui informação sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 65

(Notificação voluntária de incidentes)

1. Sem prejuízo da obrigação de notificação de incidentes prevista na presente Lei, quaisquer entidades podem notificar, ao CSIRT institucional, CSIRT Sectorial ou CSIRT Nacional, a título voluntário, os incidentes com impacto significativo na continuidade dos serviços por si prestados.

2. No tratamento das notificações voluntárias, aplica-se às disposições relativas à notificação de incidentes para os Operadores de Serviços Essenciais com as necessárias adaptações.

3. A notificação voluntária não pode dar origem à imposição à entidade notificante de obrigações às quais esta não teria sido sujeita se não tivesse procedido a essa notificação.

ARTIGO 66

(Divulgação Responsável de Vulnerabilidades)

1. A pessoa singular ou colectiva pode comunicar, publicar ou divulgar vulnerabilidades, desde que tal divulgação seja baseada na boa-fé, não sendo considerada como tendo violado as disposições legais sobre confidencialidade, integridade e disponibilidade de dados e sistemas de informação, ou que tenha incorrido em violação de leis, regulamentos, contratos e códigos de conduta profissional pelo facto de ter divulgado tais informações.

2. Para efeitos da presente Lei, considera-se que a divulgação de uma vulnerabilidade é de boa-fé, tendo em conta o seguinte:

a) se não tiver sido feita sob coacção ou ameaça de publicação de informação não tiver sido solicitada a recompensa;

b) ter sido dado um prazo razoável de, pelo menos 90 dias de calendário, para corrigir a vulnerabilidade antes de publicar ou divulgar;

c) quando no processo de identificação, a pessoa que tomou as precauções necessárias para prevenir incidentes referente à privacidade, degradação ou falhas no serviço, destruição ou manipulação dos dados;

d) se a pessoa que divulga uma vulnerabilidade considera o impacto de tal divulgação e toma os devidos cuidados para minimizar o dano que pode ser causado por tal divulgação.

3. A partir do processo de identificação de vulnerabilidades baseado na boa fé, são excluídos os métodos que possam levar à negação de serviço, evidência física, uso de código malicioso, engenharia social e alteração, remoção ou destruição de dados.

CAPÍTULO V

Fundo de Segurança Cibernética

ARTIGO 67

(Fundo)

1. É instituído pela presente Lei um Fundo de Segurança Cibernética, abreviadamente designado por (FSC) com o objectivo de prover recursos financeiros para promover e fortalecer a segurança cibernética do País.

2. O FSC é gerido pela Autoridade Nacional de Segurança Cibernética.

3. As entidades registadas e licenciadas para a prestação de serviços de TIC's devem contribuir para o FSC.

4. As regras de funcionamento do FSC são estabelecidas em regulamentação específica.

ARTIGO 68

(Objectivos do FSC)

São objectivos do FSC:

a) incrementar os recursos financeiros destinados à promoção da segurança cibernética, com vista a garantir um espaço cibernético inclusivo, seguro e resiliente;

b) providenciar recursos numa base competitiva às instituições públicas ou privadas que promovam actividades enquadradas nas linhas orientadoras estabelecidas pelo Governo em matérias de segurança cibernética;

c) promover a formação contínua para desenvolvimento de capacidade nacional em matérias de segurança cibernética.

ARTIGO 69

(Beneficiários)

São beneficiários do FSC:

a) as instituições públicas e privadas, academia e sociedade civil, em conformidade com os critérios de elegibilidade a serem definidos em regulamento específico;

b) os trabalhadores das entidades ou empresas contribuentes do FSC, através do acesso a programa de formação contínua estruturados pela empresa para actualização tecnológica em matérias de segurança cibernética;

c) as Entidades do Sistema Nacional de Segurança Cibernética contribuentes do fundo, encorajando-as a dedicar maior atenção à melhoria da qualidade dos serviços e a formação dos seus trabalhadores, como forma de melhorar a sua capacidade produtiva;

d) as entidades que pretendam estabelecer CSIRTs sectoriais e institucionais.

ARTIGO 70

(Fontes de receitas)

Constituem fontes de receitas do FSC:

a) as comparticipações e subvenções que sejam atribuídas pelo Estado e por outras pessoas colectivas do direito público;

b) as doações dos parceiros de cooperação destinadas ao financiamento da área de segurança cibernética;

c) 1% da receita bruta do ano anterior das Entidades do Sistema Nacional de Segurança Cibernética, licenciadas no âmbito do exercício da actividade de prestação de serviços de segurança cibernética;

d) outras fontes de receitas ou financiamento que lhe vierem a ser destinados.

ARTIGO 71

(Gestão)

A Autoridade Nacional de Segurança Cibernética é responsável pela gestão do FSC, de acordo com a Legislação Orçamental.

CAPÍTULO VI

Supervisão, Fiscalização, Contravenções e Sanções

ARTIGO 72

(Supervisão)

Compete a Autoridade Nacional de Segurança Cibernética garantir a realização da supervisão nos sectores abrangidos pela presente Lei.

ARTIGO 73

(Fiscalização)

Compete a Autoridade Nacional de Segurança Cibernética realizar acções de fiscalização das actividades em matéria de segurança cibernética.

ARTIGO 74

(Auditoria)

A Autoridade Nacional de Segurança Cibernética estabelece os padrões técnicos que servem de base para realização de auditoria de segurança cibernética e de segurança de informação, nos termos a regulamentar.

ARTIGO 75

(Contravenções)

Constituem contravenções à presente Lei:

a) a violação da responsabilidade do responsável de uma Infra-estrutura Crítica de informação registada de notificar a Autoridade Nacional de Segurança Cibernética no prazo de 7 dias, a contar da mudança de propriedade legal da Infra-estrutura Crítica de informação registada;

b) a falha do responsável de uma Infra-estrutura Crítica de informação em relatar um incidente de segurança cibernética;

c) a recusa ou obstrução da investigação do responsável de uma infra-estrutura de informação crítica em fazer com que uma auditoria seja realizada na infra-estrutura de informação crítica;

d) a recusa do responsável de uma Infra-estrutura Crítica de informação em apresentar uma cópia do relatório de auditoria à Autoridade de Segurança Cibernética;

e) o incumprimento das directrizes regulatórias emanada pela Autoridade Nacional de Segurança Cibernética;

f) a recusa da instituição em relatar um incidente de segurança cibernética ao órgão competente;

g) a violação do dever de licenciar os serviços previstos na presente Lei;

h) o uso intencional de uma licença não concedida ao Provedor de Serviço;

i) o incumprimento dos requisitos e medidas de segurança cibernética;

j) a utilização indevida, por parte do Provedor de Serviços, de mecanismos ou recursos de interceptação na execução de um mandado de interceptação emitido por tribunal de jurisdição competente;

k) a omissão, pelo Provedor de Serviços, da adopção das medidas necessárias para permitir a desencriptação de uma comunicação de telecomunicações, nos termos de um mandado de interceptação emitido pelo tribunal competente;

l) o incumprimento, pelo Provedor de Serviços, da obrigação de reter as informações do assinante pelo período de um ano;

m) o incumprimento, pelo Provedor de Serviços, da obrigação de reter os dados de tráfego pelo período de um ano;

n) a violação da responsabilidade do Provedor de Serviços em não reter dados de tráfego por um período de um ano;

o) o uso ilegal de dados retidos para uma finalidade diferente da declarada em um mandado de interceptação;

p) a violação de obrigação do responsável ou Operador de uma Infra-estrutura Crítica de informação, um CSIRT designado ou um Provedor de Serviço Digital em apresentar informações relevantes à Autoridade Competente;

q) a recusa do Provedor de Serviços em cumprir com uma decisão da Autoridade Nacional de Segurança Cibernética para bloquear, filtrar ou remover qualquer conteúdo que ameaça ou afecta a segurança cibernética do País;

r) o incumprimento de uma directiva emanada pela Autoridade Nacional de Segurança Cibernética;

s) o incumprimento diário por parte do responsável de uma Infra-estrutura de informação Crítica, do CSIRT designado ou de um prestador de serviço digital em cumprir um pedido de envio de informação relevante a Autoridade Competente com a finalidade de garantir a segurança cibernética do País;

t) o incumprimento da obrigação de requisitos de segurança previstos nos artigos 48, 50, 51, 52, 53, 54, 55 e 56, da presente Lei.

u) o incumprimento da obrigação de notificação de incidentes de segurança previsto nos artigos 58, 59, 60, 61, 62, 63, 64 e 65, da presente Lei.

v) o incumprimento das instruções e alertas de segurança cibernética emitidas pela Autoridade Nacional de Segurança Cibernética previsto na alínea *h),* do artigo 11, da presente Lei.

w) todos os factos ilícitos que preencham um tipo legal correspondente à violação de disposições legais relativas à segurança cibernética para as quais, caiba multa, suspensão de licenças, certificados, autorizações ou proibição de operação ou sanção estabelecidas em legislação específica.

ARTIGO 76

(Sanções)

Sem prejuízo de aplicação da pena mais grave no âmbito da legislação penal, as infracções previstas no presente artigo são puníveis, nos seguintes termos:

a) a violação do disposto na alínea *h),* do artigo 75, da presente Lei é punível com a multa de 35 salários mínimos em vigor na Função Pública;

b) a violação do disposto na alínea *q),* do artigo 75, da presente Lei é punível com a multa de 2 a 17 salários mínimos em vigor na Função Pública;

c) a violação do disposto nas alíneas *j)* e *k),* do artigo 75, da presente Lei é punível com a multa de 7 salários mínimos em vigor na Função Pública;

d) a violação do disposto nas alíneas *a), b), c), d), l), m), n), o), p)* e *s)* do artigo 75, da presente Lei é punível com a multa de 1 a 7 salários mínimos em vigor na Função Pública;

e) a violação do disposto nas alíneas *e), f)* e *i),* do artigo 75, em vigor na da presente Lei é punível com a multa de 1 a 4 salários mínimos em vigor na Função Pública;

f) a violação do disposto nas alíneas *r)* e *t),* do artigo 75, da presente Lei é punível com a multa de 1 salário mínimo da Função Pública por semana;

g) a violação do disposto na alínea *g),* do artigo 75 da presente Lei é punível com a multa de 64 salários mínimos em vigor na Função Pública;

h) a violação da obrigação de requisitos de segurança previsto nos artigos 48, 50, 51, 52, 53, 54, 55 e 56, da presente Lei é punível com uma multa de 90 a 160 salários mínimos em vigor na Função Pública;

i) a violação da obrigação de notificação de incidentes de segurança previsto nos artigos 58, 59, 60, 61, 62, 63, 64 e 65, da presente Lei é punível com a multa de 80 a 100 salários mínimos em vigor na Função Pública;

j) a violação da observância das instruções e alertas de segurança cibernética emitidas pela Autoridade Nacional de Segurança Cibernética tal como previsto na alínea *h),* do artigo 11, da presente Lei é punível com a multa de 60 a 90 salários mínimos em vigor na Função Pública.

CAPÍTULO VII

Disposições finais

ARTIGO 77

(Regime subsidiário)

É aplicável subsidiariamente à presente Lei, em tudo que se mostre omisso, o regime jurídico aplicável às transacções electrónicas e demais legislação complementar.

ARTIGO 78

(Unidades Especializadas em Operações Cibernéticas)

1. As unidades especializadas em operações cibernéticas para as actividades de defesa nacional, segurança interna e segurança do Estado são criadas para prestarem serviços de defesa e segurança cibernética, e para fins de defesa nacional.

2. As unidades especializadas em operações cibernéticas trabalham em coordenação com o Centro de Coordenação Cibernética das Forças de Defesa e Segurança.

ARTIGO 79

(Regulamentação)

1. As matérias de Segurança Cibernética relacionadas com as actividades de defesa nacional, segurança interna e segurança do Estado são estabelecidas em regulamentação específica.

2. Compete ao Conselho de Ministros regulamentar a presente Lei no prazo de 180 dias a contar da data da sua publicação.

ARTIGO 80

(Entrada em vigor)

A presente Lei entra em vigor 90 dias após a sua publicação.

Aprovada pela Assembleia da República, aos 29 de Abril de 2026.

A Presidente da Assembleia da República, *Margarida Adamugi Talapa.*

Promulgada, aos 10 de Junho de 2026.

Publique se.

O Presidente da República, DANIEL FRANCISCO CHAPO.

Anexo I

Glossário

A

Activo de Informação – todo elemento que agrega valor ao negócio podendo ser uma informação digital ou física, *hardware, software,* pessoa ou ambiente físico, meios de armazenamento, transmissão e processamento bem como os sistemas de informação, cuja quebra da confidencialidade, integridade ou disponibilidade trará prejuízo.

Ameaça Cibernética – qualquer factor ou acção capaz de interferir e causar danos à integridade, à confidencialidade, à autenticidade e à disponibilidade de dados e informações numa organização.

C

Crime cibernético – é todo o acto em que os sistemas de computadores, redes, dispositivos electrónicos e dados servem de meio para atingir um objectivo criminoso.

D

Defesa cibernética – refere-se ao conjunto de medidas, estratégias, políticas e tecnologias adoptadas para proteger sistemas de computadores, redes, dispositivos e dados contra ameaças cibernéticas.

E

Engenharia social – é o acto de manipular uma pessoa através de técnicas psicológicas e habilidades sociais para atingir objectivos específicos.

Equipa de Resposta a Incidentes de Segurança Cibernética (CSIRT) – a equipa que actua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação.

Espaço cibernético – espaço não físico, criado por redes de comunicações, onde as pessoas podem comunicar.

I

Infraestrutura crítica – a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções.

O

Operador de Rede de Infra-estruturas Críticas – é uma entidade pública ou privada responsável pela gestão, operação e manutenção de sistemas e activos essenciais (como energia, transportes, água e comunicações).

Operador de Rede de Serviços Essenciais – é uma entidade pública ou privada que fornece serviços cruciais, cuja interrupção impacta gravemente a saúde, segurança ou economia.

Operadores de plataformas digitais – entidades que gerem infraestruturas baseadas na *Internet* e aplicações, conectando fornecedores de serviços ou produtos a clientes finais.

Operadores de comunicações electrónicas – são entidades que fornecem redes, serviços de telefonia, *Internet,* televisão e transmissão de dados através de infraestruturas físicas (fibra, satélite, torres) ou virtuais.

P

Prestador de serviços do sistema de nomes de domínio – uma entidade que presta serviços do sistema de nomes de domínio (DNS) na *Internet*.

Provedor Intermediário de Serviço de *"mera conduta"* – consiste na transmissão de informações fornecidas por um destinatário do serviço numa rede de comunicações ou no fornecimento de acesso a uma rede de comunicações.

Provedor Intermediário de Serviço de *"caching"* – consiste na transmissão numa rede de comunicações de informação fornecida por um destinatário do serviço, envolvendo o armazenamento automático, intermédio e temporário dessa informação, com o único objectivo de tornar mais eficiente a transmissão posterior da informação a outros destinatários mediante solicitação.

Provedor Intermediário de Serviço de "hospedagem" – consiste no armazenamento de informações fornecidas por e a pedido de um destinatário do serviço.

Provedores de Serviços de Segurança Cibernética – são entidades privadas que monitoram, gerenciam e protegem a infraestrutura de Tecnologias de Informação, redes e dados de outras organizações, oferecem vigilância contínua, detecção de ameaças e resposta a incidentes.

Provedores de Serviços Digitais – entidades que oferecem acesso, armazenamento, processamento ou transmissão de dados e conteúdos via *Internet*.

Provedores Intermediários de Serviços – qualquer pessoa que, em representação de outra pessoa, envia, recebe ou armazena mensagens de dados. São aqueles que prestam serviço de acesso à rede ou que prestam serviços a partir dela (provedores de acesso, provedores de conteúdos, provedores de aplicativos e provedores de hospedagem).

R

Rede e sistema de informação – é o conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações electrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção.

S

Segurança Cibernética – é o conjunto de políticas, conceitos de segurança, ferramentas, garantias de segurança, directrizes, abordagens de gestão de risco, acções, capacitações, boas práticas, que podem ser usadas para proteger o ambiente cibernético e activos das pessoas e organizações.

Segurança das redes e dos sistemas de informação – a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a acções que comprometam a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles.

Serviço essencial – um serviço essencial para a manutenção de actividades sociais ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço.

Serviços digitais – são serviços oferecidos por meio electrónicos, em que todas as informações são transmitidas e acedidas por meio de uma rede de dados, como a *Internet*.

Sistema de informação – é o conjunto organizado de recursos humanos, tecnológicos, processos e dados, utilizado para recolher, processar, gerir e disseminar informações de forma a apoiar a tomada de decisões, a coordenação, o controle e a análise em uma organização.

Sistema de nomes de domínio (DNS) – um sistema de nomes distribuídos hierarquicamente numa rede que encaminha pesquisas sobre nomes de domínio.

T

Tratamento de incidentes – todos os procedimentos de apoio à detecção, análise, contenção e resposta a um incidente.

V

Vulnerabilidade – qualquer fragilidade em um sistema de informação, seus procedimentos de segurança, sua implementação ou em seus controles interno, o que poderia permitir a materialização de uma ameaça.

Anexo II

Sectores, subsectores e tipos de entidades dos operadores de serviços essenciais

#	Sector	Subsector	Tipo de Entidade
1	Energia	Electricidade	Empresa de electricidade que exerce a actividade de produção ou de comercialização.
			Operadores da rede de distribuição.
			Operadores da rede de transporte.
		Petróleo	Operadores de oleodutos de petróleo.
			Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo.
		Gás	Empresas de comercialização.
			Operadores da rede de distribuição.
			Operadores da rede de transporte.
			Operadores do sistema de armazenamento.
			Operadores da rede de gás natural em estado líquido (GNL).
			Empresas de gás natural.
			Operadores de instalações de refinamento e tratamento de gás natural.
2	Água	Fornecimento e distribuição de água potável.	Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua actividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais.
		Colecta e Tratamento de Águas Residuais	
		Retenção de águas	Sistemas de Retenção de águas.
3	Transportes	Transporte aéreo	Transportadoras aéreas, companhias, agentes, operadores.
			Entidades gestoras aeroportuárias, aeroportos e as entidades que exploram instalações anexas existentes dentro dos aeroportos.
			Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo.
		Transporte marítimo e por Vias navegáveis interiores	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias.
			Entidades gestoras dos portos, incluindo as respectivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos.
			Operadores de serviços de tráfego marítimo.

#	Sector	Subsector	Tipo de Entidade
3	Transportes	Transporte terrestres	Autoridades rodoviárias e ferroviárias.
			Transportadores, companhias, agentes e operadores
			Operadores de serviço de tráfego rodoviário e ferroviário
			Operadores de sistemas de transporte inteligentes.
4	Finanças	Banca	Instituições de crédito.
		Seguros	
		Bolsa e Valores	Operadores de plataformas de negociação.
5	Infra-estruturas do mercado financeiro		Contrapartes centrais.
6	Saúde	Instalações de prestação de cuidados de saúde	Prestadores de cuidados de saúde.
		Instalações de Controlo e Logística	Armazéns de Medicamentos Prestadores de serviços de distribuição de Medicamentos
7	Infra-estruturas de Telecomunicações		Operadoras de Telecomunicações
8	Infra-estruturas de *Internet*		Registos de nomes de domínio de topo
			Pontos de troca de tráfego (IXP).
			Prestadores de serviços de Sistema de Nomes de Domínio (Domínio .MZ)
			Provedores de Serviços de *Internet*
			Rede Tecnológica Privada do Estado

ASSEMBLEIA DA REPÚBLICA

Lei n.º 14/2026

de 1 de Julho

Havendo necessidade de estabelecer o regime jurídico dos crimes cibernéticos com vista a assegurar a protecção, a recolha de prova e a responsabilização criminal, visando garantir a cooperação internacional sobre a matéria, ao abrigo do disposto no número 1 do Artigo 178, da Constituição da República, a Assembleia da República, determina:

CAPÍTULO I

Disposições Gerais

ARTIGO 1

(Objecto)

A presente Lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal no domínio dos crimes cibernéticos e da recolha de prova em suporte electrónico.

ARTIGO 2

(Âmbito de aplicação)

A presente Lei aplica-se a todas as pessoas singulares e colectivas, públicas ou privadas, que utilizam redes de comunicação de dados e sistemas de informação.

ARTIGO 3

(Definições)

As definições dos termos e expressões utilizadas na presente Lei, constam do Glossário em anexo que dela é parte integrante.

CAPÍTULO II

Disposições Penais Materiais

ARTIGO 4

(Acesso ilegítimo)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito sobre o sistema ou de parte dele, se introduzir num dispositivo alheio, fixo ou móvel, ligado ou não à rede de computadores, com o fim de obter informação não pública de correio ou comunicações electrónicas privadas, acesso a dados privados, segredos comerciais ou industriais, informações sigilosas ou o acesso remoto não autorizado ao dispositivo é punido com pena de prisão de 1 a 2 anos e multa até 1 ano.

2. Na mesma pena incorre quem, ilegitimamente, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número 1 do presente artigo.

3. Para efeitos do disposto nos números 1 e 2 do presente artigo, o procedimento criminal não depende de queixa, salvo quando estejam em causa dados relativos à vida privada.

ARTIGO 5

(Intercepção ilegítima)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito sobre o sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão de até 3 anos e multa de até dois anos.

2. Incorre na mesma pena quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos, dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número 1 do presente artigo.

ARTIGO 6

(Interferência em dados)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular sobre o sistema ou de parte dele, alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, alterar dados informáticos, é punido com pena de prisão de 1 a 2 anos e multa correspondente.

2. Quem, mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, instalar vulnerabilidades, interferir no funcionamento de sistema informático, causando intencionalmente dano à infra-estrutura crítica, ou interrupção de fornecimento de serviços críticos, é punido com pena de prisão de 3 anos e multa correspondente.

ARTIGO 7

(Interferência em sistemas)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito sobre o sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, eliminação, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 2 anos e multa até 1 ano.

2. À mesma infracção é aplicada a pena de prisão de 3 anos e multa correspondente, se a acção for praticada contra infra-estruturas, ou serviços críticos.

3. Se da conduta resultar dano relevante, afectação de serviços essenciais ou prejuízo significativo para terceiros, o agente é punido com pena de prisão de 2 a 8 anos.

ARTIGO 8

(Uso abusivo de dispositivos)

Quem, ilegitimamente, produzir, vender, distribuir, importar ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nos artigos 4 e 5, da presente Lei, é punido com pena de prisão de 1 a 2 anos.

ARTIGO 9

(Falsidade informática)

1. Quem introduzir, modificar, apagar ou suprimir de forma intencional e ilegítima dados informáticos, produzindo dados ou documentos falsos ou não genuínos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se o fossem, é punido com pena de prisão de 1 a 5 anos e multa até 1 ano.

2. Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no número 1 do presente artigo, ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número 1, do presente artigo, é punido com as penas previstas nos números 1 e 3, do presente artigo.

3. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções previstas nos números anteriores, é punido com pena de prisão de 2 a 8 anos.

4. A pena referida no número 1, do presente artigo, é também aplicável a quem, com objectivo de tirar proveito, manipular, falsificar ou usar indevidamente a identidade de outrém.

5. A ocorrência de danos morais ou patrimoniais em qualquer dos casos previstos no presente artigo constitui circunstância agravante.

ARTIGO 10

(Burla informática e nas comunicações)

1. Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão de até 3 anos e multa correspondente.

2. A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.

ARTIGO 11

(Espionagem cibernética)

1. Quem aceder, ilicitamente ou sem autorização, ao sistema informático governamental para a obtenção de informações classificadas ou estratégicas, com motivações políticas, económicas ou militares, para fins de inteligência estrangeira, é punido com pena de prisão de 3 a 10 anos.

2. Quem invadir redes corporativas para apropriação de segredos industriais ou estratégias comerciais e comprometimento de infra-estruturas críticas e serviços críticos, é punido com a pena de 2 a 8 anos.

ARTIGO 12

(Terrorismo e extremismo violento cibernéticos)

1. Quem atacar ou ameaçar atacar, invadir ou ameaçar invadir, destruir ou adulterar dados ou sistemas informáticos de infra-estruturas críticas, perturbando total ou parcialmente o seu funcionamento ou o fornecimento de seus serviços, é punido com pena de prisão de 2 a 8 anos.

2. É punido com a mesma pena de prisão prevista no número 1 do presente artigo, quem mobilizar ou recrutar, produzir e difundir conteúdos, através do sistema informático, com motivações políticas, económicas e religiosas, visando causar pânico, medo ou terror.

ARTIGO 13

(Extorsão cibernética)

1. Quem ameaçar divulgar informações comprometedoras, ataques a sistemas informáticos, ou vazamento de dados pessoais no espaço digital em troca de pagamento, é punido com a pena de prisão até 2 anos e multa correspondente.

2. A infracção referida no número 1 do presente artigo é punida com a pena de prisão de até 3 anos e multa correspondente, quando a vítima se tratar de titular ou membro de órgão de soberania, membro do governo, titular de órgão público e titular de órgão de Administração da Justiça.

ARTIGO 14

(Punição da tentativa)

A tentativa de prática dos ilícitos previstos na presente Lei é punível nos termos do Código Penal.

ARTIGO 15

(Conteúdo sexual infantil no ambiente digital)

1. Quem produzir, oferecer, trocar, disponibilizar, transmitir ou publicar, por meio de sistema informático ou telemático, fotografia, vídeo ou outro registo que contenha conteúdo sexual ou pornográfico envolvendo menores de idade, é punido com uma pena de prisão de 6 meses a 1 ano e multa até 1 ano.

2. O disposto no número 1 do presente artigo, não se aplica à aquele que praticar o acto previsto, com a finalidade de comunicar às autoridades competentes sobre a ocorrência do facto.

ARTIGO 16

(Responsabilidade penal das pessoas colectivas e entidades equiparadas)

As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente Lei, nos termos e limites do respectivo regime de responsabilização previstos no Código Penal.

CAPÍTULO III

Disposições Processuais

ARTIGO 17

(Âmbito de aplicação das disposições processuais)

As disposições processuais previstas no presente Capítulo aplicam-se à investigação dos seguintes crimes:

a) previstos na presente Lei;

b) cometidos por meio de um sistema informático;

c) que impliquem a recolha de prova em suporte digital.

ARTIGO 18

(Preservação expedita de dados)

1. Se, no decurso do processo, for necessário para efeitos de obtenção da prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente ao fornecedor de serviço, que preserve e proteja os dados em causa.

2. A preservação pode também ser ordenada pelo órgão de investigação criminal mediante autorização prévia da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, comunicar imediatamente o facto à autoridade judiciária competente.

3. A ordem de preservação discrimina, sob pena de nulidade:

a) a natureza dos dados;

b) a sua origem e destino, se forem conhecidos;

c) o prazo pelo qual os dados devem ser preservados até ao máximo de três meses.

4. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5. A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c),* do número 3 do presente artigo, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de 1 ano.

ARTIGO 19

(Revelação expedita de dados de tráfego)

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo 18, da presente Lei, indica a autoridade judiciária ou o órgão de investigação criminal, assim que tiver conhecimento, outros fornecedores de serviço, através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

ARTIGO 20

(Injunção para apresentação ou concessão do acesso a dados)

1. Se no decurso do processo se tornar necessário reunir elementos de prova, tendo em vista a descoberta da verdade, para a obtenção de dados informáticos específicos e determinados, armazenados num determinado sistema informático ou num dispositivo de armazenamento de dados informáticos, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os apresente ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

2. A ordem referida no número 1 do presente artigo deve identificar os dados em causa.

3. Em cumprimento da ordem descrita nos números 1 e 2 do presente artigo aquele que tiver disponibilidade ou controlo desses dados apresenta-os à autoridade judiciária competente ou permite, sob pena de prática do crime de desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4. O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que juntem ao processo dados relativos aos seus clientes ou assinantes ou qualquer outra informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:

a) o tipo de serviço de comunicação utilizado, as medidas técnicas adoptadas a esse respeito e o período de serviço;

b) a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;

c) qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5.Os pedidos referidos no número 4 do presente artigo podem ser dirigidos e enviados directamente a um prestador de serviços estrangeiro, no âmbito de tratados internacionais que vinculem Moçambique, sempre que os dados solicitados sejam necessários para a obtenção da prova de prática de crimes.

6. Do mesmo modo, a ordem descrita no presente artigo é aplicável a entidades que prestam serviços de registo de nomes de domínio a fim de identificar ou contactar o titular registado de um nome de domínio.

7. A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo, nem a pessoa que validamente possa recusar-se a depor.

8. Não pode igualmente fazer-se uso da injunção prevista no presente artigo quanto a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária.

ARTIGO 21

(Pesquisa de dados informáticos)

1. Quando no decurso do processo se tornar necessário para a prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2. O despacho previsto no número 1 do presente artigo tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3. O órgão de investigação criminal pode proceder à pesquisa, sem prévia autorização da competente autoridade judiciária, quando:

a) a mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) nos casos de terrorismo e criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4. Quando o órgão de investigação criminal proceder à pesquisa nos termos do número 3 do presente artigo, a realização da diligência é, sob pena de nulidade, logo que seja possível comunicar à autoridade judiciária competente e por esta apreciada em ordem à sua validação.

5. Quando, no decurso da pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida, mediante autorização ou ordem da autoridade judiciária competente, nos termos dos números 1 e 2, do presente artigo.

6. À pesquisa a que se refere o presente artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas, nos termos do Código de Processo Penal.

ARTIGO 22

(Apreensão de dados informáticos)

1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados, mensagens de correios electrónicos ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade material, a autoridade judiciária competente autoriza ou ordena, por despacho, a apreensão dos mesmos.

2. O órgão de investigação criminal pode efectuar apreensões, sem prévia autorização da competente autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 21 da presente Lei, bem como quando haja urgência ou perigo na demora.

3. Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados privados ou íntimos que possam pôr em causa a privacidade do respectivo titular, ou de terceiro, sob pena de nulidade, esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

4. As apreensões efectuadas pelo órgão de investigação criminal são sempre sujeitas à validação pela autoridade judiciária competente, no prazo máximo de 72 horas.

5. A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:

a) apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;

b) realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos;

d) eliminação não reversível ou bloqueio do acesso aos dados.

ARTIGO 23

(Intercepção de comunicações)

1. É admissível o recurso à intercepção de comunicações em processos relativos a crimes previstos na presente Lei, bem como quanto a crimes que se encontrem previstos no artigo 222 do Código de Processo Penal, quando cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

2. A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho judicial especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

3. À intercepção e registo de transmissões de dados informáticos aplica-se o regime da intercepção e gravação de conversações ou comunicações telefónicas, previsto no Código de Processo Penal.

ARTIGO 24

(Acções encobertas)

É admissível o recurso às acções encobertas previstas no artigo 227 do Código de Processo Penal na investigação dos crimes previstos na presente Lei e dos demais crimes cometidos com recurso à tecnologia informática, desde que puníveis com pena de prisão igual ou superior a 2 anos.

CAPÍTULO IV

Cooperação Internacional

ARTIGO 25

(Âmbito da cooperação internacional)

As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de prevenção, investigação ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um determinado crime.

ARTIGO 26

(Informação espontânea)

1. Quando, no decurso de um processo, se obtiverem informações que possam ser úteis ao início de uma investigação criminal, ou a uma investigação criminal já existente, noutro Estado, a autoridade judiciária competente comunica tais informações à Autoridade Central, que por sua vez as comunica à Autoridade Central desse outro Estado.

2. Se as exigências do caso pendente na República de Moçambique assim o determinarem, tal comunicação pode ser acompanhada da solicitação de que as mesmas permaneçam confidenciais ou apenas sejam utilizadas em determinadas condições.

3. Para efeitos do número 2 do presente artigo, a Autoridade Central certifica-se, previamente, junto da Autoridade Central do outro Estado, que este pode satisfazer esta solicitação, apenas sendo as informações efectivamente remetidas neste caso.

ARTIGO 27

(Ponto de contacto permanente para a cooperação internacional)

1. Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata a investigações e procedimentos respeitantes a infracções penais previstas no artigo 16 da presente Lei, é assegurada pelo Ministério Público a manutenção de uma estrutura que garante um ponto de contacto disponível em regime de permanência.

2. Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Moçambique se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais.

3. A assistência imediata prestada por este ponto de contacto permanente inclui:

a) a prestação de aconselhamento técnico a outros pontos de contacto;

b) a preservação expedita de dados nos casos de urgência ou perigo na demora;

c) a recolha de prova para a qual seja competente nos termos da lei processual penal, nos casos de urgência ou perigo na demora;

d) a localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora;

e) em caso de emergência, no quadro de tratados ou acordos internacionais que vinculem Moçambique, receber pedidos de um outro ponto de contacto, pelo qual se solicite assistência imediata para obter, de forma expedita e sem pedido formal de auxílio judiciário mútuo, dados informáticos específicos armazenados, na posse ou sob o controlo de um prestador de serviços em Moçambique.

4. Sempre que actue ao abrigo das alíneas *b)* e *c),* do número 3 do presente artigo, o órgão de investigação criminal comunica, de imediato, ao Ministério Público, remetendo o respectivo relatório nos termos do Código de Processo Penal.

ARTIGO 28

(Preservação e revelação expeditas de dados informáticos em cooperação internacional)

1. Pode ser solicitada à República de Moçambique a preservação expedita de dados informáticos armazenados em sistema informático localizado no seu território, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2. A solicitação especifica:

a) a autoridade que pede a preservação;

b) a infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados;

c) os dados informáticos a conservar e a sua relação com a infracção;

d) todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático;

e) a necessidade da medida de preservação;

f) a intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados.

3. Em execução da solicitação de autoridade estrangeira competente, nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente ao fornecedor de serviço, que os preserve.

4. A preservação pode também ser ordenada pelo órgão de investigação criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora.

5. A ordem de preservação especifica, sob pena de nulidade:

a) a natureza dos dados;

b) se forem conhecidos, a origem e o destino dos mesmos;

c) o período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses.

6. Em cumprimento da ordem de preservação que lhe seja dirigida, aquele que tiver disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, pelo período de tempo especificado, protegendo e conservando a sua integridade.

7. A autoridade judiciária competente, ou o órgão de investigação criminal, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c),* do número 5, do presente artigo, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de 1 ano.

8. Quando seja apresentado o pedido de auxílio referido no número 1, do presente artigo, a autoridade judiciária competente para dele decidir, determina a preservação dos dados até à adopção de uma decisão final sobre o pedido.

9. Os dados preservados ao abrigo do presente artigo, apenas podem ser fornecidos:

a) à autoridade judiciária competente, em execução do pedido de auxílio referido no número 1, do presente artigo, nos mesmos termos em que poderiam sê-lo, em caso de pedido nacional semelhante;

b) à autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante.

10. A autoridade nacional à qual, nos termos do número 9 do presente artigo, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via, através dos quais a comunicação foi efectuada, comunica-os imediatamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.

11. O disposto nos números 1 e 2 do presente artigo, aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades moçambicanas.

ARTIGO 29

(Motivos de recusa)

1. Para além dos motivos que em geral podem fundamentar a recusa de cooperação jurídica e judiciária internacional, a solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando:

a) os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do Direito moçambicano;

b) atentar contra a soberania, segurança, ordem pública ou outros interesses da República de Moçambique, constitucionalmente consagrados;

c) o Estado requerente não oferecer garantias adequadas de protecção dos dados pessoais.

2. A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados pode ser recusado por ausência de verificação do requisito da dupla incriminação.

ARTIGO 30

(Acesso a dados informáticos em cooperação internacional)

1. Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Moçambique, nos mesmos termos e condições em que a pesquisa e apreensão sejam admissíveis em caso de pedido nacional semelhante.

2. A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em acordo internacional aplicável.

3. O disposto no número 1 do presente artigo, aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias moçambicanas.

ARTIGO 31

(Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento)

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades moçambicanas, podem:

a) aceder a dados informáticos armazenados em sistema informático localizado em Moçambique, quando publicamente disponíveis;

b) receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Moçambique, mediante consentimento voluntário de pessoa legalmente autorizada a divulgar.

ARTIGO 32

(Intercepção de comunicações electrónicas em cooperação internacional)

A realização de intercepção de comunicações solicitada pelas competentes autoridades estrangeiras, no contexto de investigações de crimes previstos na presente Lei, é efectuada nos termos descritos no artigo 157, da Lei n.º 21/2019, de 11 de Novembro, Lei da Cooperação Jurídica e Judiciária Internacional em Matéria Penal.

CAPÍTULO V

Disposições Transitórias e Finais

ARTIGO 33

(Regime subsidiário)

Em tudo o que não contrarie o disposto na presente Lei, aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, aplicam-se, respectivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei n.º 21/2019, de 11 de Novembro, Lei da Cooperação Jurídica e Judiciária em Matéria Penal.

ARTIGO 34

(Revogação)

1. São revogados os artigos 256, 289, 336, 337, 338 e 339, do Código Penal, aprovado pela Lei n.º 24/2019, de 24 de Dezembro, alterada pela Lei n.º 17/2020, de 23 de Dezembro.

2. São revogados o artigo 57 e o número 2 do artigo 66, ambos da Lei n.º 4/2016, de 3 de Julho, Lei das Telecomunicações.

ARTIGO 35

(Regulamentação)

Sem prejuízo das competências conferidas a determinadas entidades, compete ao Conselho de Ministros regulamentar a presente Lei, no prazo de 180 dias, a contar da data da sua publicação.

ARTIGO 36

(Entrada em vigor)

A presente Lei entra em vigor 90 dias, após a sua publicação.

Aprovada pela Assembleia da República, aos 29 de Abril de 2026.

A Presidente da Assembleia da República, *Margarida Adamugi Talapa.*

Promulgada, aos 10 de Junho de 2026.

Publique se.

O Presidente da República, DANIEL FRANCISCO CHAPO.

Preço — 120,00MT

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.