Proposta de Lei

Versão 6.0

15/09/2023

República de Moçambique

Assembleia da República

Lei n.º /2023

De de

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 cidadão, das instituições, do Estado e a protecção de sistemas de informação e infra-estruturas críticas no espaço cibernético, ao abrigo do disposto do 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 cidadão, das instituições e do Estado, bem como assegurar a protecção de redes de comunicação de dados, de dados, de sistemas de informação e de infra-estruturas críticas no espaço cibernético.

ARTIGO 2

(Âmbito)

1. A presente Lei aplica-se a:

a) Administração Pública;
b) Operador de Rede de Infra-estruturas Críticas;
c) Provedores Intermediários de Serviços;
d) Provedores de Serviços Digitais;

e) Operador de Rede de Serviços Essenciais;
f) Provedores de Serviços de Segurança Cibernética;
g) Operadores de plataformas digitais;
h) Operadores de comunicações electrónicas.
i) a quaisquer outras entidades que utilizam redes de comunicação de dados e sistemas de informação.

2. Exceptuam-se do previsto no número 1 do presente artigo, as seguintes redes:

a) redes de comunicação de dados e sistemas de informação directamente relacionados com o comando e controlo das entidades que superintendem as Forças de Defesa e Segurança;
b) 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)

Para efeitos da presente Lei, as definições dos termos e acrónimos, constam do glossário em anexo, que dela é parte integrante.

ARTIGO 4

(Princípios)

A presente lei rege-se pelos seguintes princípios:

a) Colaboração: consiste na implementação de medidas para assegurar a estabilidade, aumentar segurança e evitar práticas consideradas prejudiciais ou susceptíveis de pôr em perigo o uso das Tecnologias de Informação e Comunicação (TIC);
b) Cooperação: consiste na troca de informação, assistência mútua interinstitucional e entre Estados, no âmbito de ameaças e incidentes de segurança cibernética;
c) 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;
d) 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 apoio de Tecnologias de Informação e Comunicação;
e) Transparência: o Estado deve assegurar a não proliferação de inovações, técnicas e instrumentos maliciosos, bem como o uso de funções ocultas e prejudiciais no domínio das Tecnologias de Informação e Comunicação;

f) Divulgação de vulnerabilidades: encorajar a divulgação responsável de vulnerabilidades de segurança cibernética;
g) Responsabilidade: consiste na abstenção de produção ou uso de soluções prejudiciais ao ecossistema tecnológico.

CAPÍTULO II

Organização do Sistema de Segurança Cibernética

SECÇÃO I

Estrutura do sistema de segurança cibernética

ARTIGO 5

(Segurança Cibernética)

A Segurança Cibernética é o conjunto de ferramentas, políticas, conceitos de segurança, 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.

ARTIGO 6

(Estrutura)

O Sistema 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; e
   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;
   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; e
   ix. Provedores de Serviços de Segurança Cibernética;
   x. Operadores de Comunicações Digitais.

Subsecção I

Conselho Nacional de Segurança Cibernética

ARTIGO 7

(Natureza)

O Conselho Nacional de Segurança Cibernética, abreviadamente designado por CNSC é o órgão multissectorial de coordenação e de governação específica para assuntos relativos a Segurança Cibernética e, é presidido pelo Ministro que superintende a área de Tecnologias de Informação e Comunicação.

ARTIGO 8

(Composição)

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

a) Representantes dos sectores que superintendem:

i. as Forças de Defesa e Segurança;
ii. a área de Tecnologias de Informação e Comunicação;
iii. a área de Justiça;
iv. a área de Comunicações;
v. a área de Economia e Finanças;
vi. a área de Negócios Estrangeiros e Cooperação;
vii. a área de Educação;
viii. a área de Saúde;
ix. a área do Género;
x. a área da Criança;
xi. a área de Energia;
xii. a área de Transportes;
xiii. a área de Água.

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 Medicamentos;
vii. Regulador do Sector de Investigação Científica em Saúde Humana;
viii. Serviço Nacional de Investigação Criminal;
ix. Equipa Nacional de Resposta a Incidentes de Segurança Cibernética (CSIRT Nacional);

x. Conselho Nacional de Ética na Investigação Científica;
xi. Embaixador Itinerante para a área de TIC.

2. Sempre que se mostre necessário, desde que devidamente fundamentada a pertinência, podem ser convidados 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) verificar a implementação da Estratégia Nacional de Segurança Cibernética;
c) pronunciar-se sobre a Estratégia Nacional de Segurança Cibernética previamente à sua submissão para aprovação;
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 as solicitações por parte do Governo, no âmbito das suas competências.

Subsecção II

Autoridade Nacional de Segurança Cibernética

ARTIGO 10

(Natureza)

1. A Autoridade Nacional de Segurança Cibernética é uma instituição pública, dotada de personalidade jurídica, autonomia administrativa, financeira e patrimonial.

2. A Entidade Reguladora de Tecnologias de Informação e Comunicação exerce as funções de Autoridade Nacional de Segurança Cibernética.

ARTIGO 11

(Competências)

Compete à Autoridade Nacional de Segurança Cibernética:

a) exercer as funções de regulação, supervisão, fiscalização e sancionatórias no âmbito da segurança cibernética;
b) 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;
c) registar e licenciar os Provedores de Serviços de Segurança Cibernética;
d) auditar as Entidades do Sistema de Segurança Cibernética;
e) 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;
f) credenciar profissionais de segurança cibernética;
g) definir e implementar medidas e instrumentos necessários à antecipação, detecção, reacção e recuperação de situações que, face à iminência e ocorrência de incidentes cibernéticos que ponham em causa o interesse nacional;
h) propor ao Governo a actualização da lista de serviços essenciais;
i) garantir a protecção de infra-estruturas críticas em coordenação com as entidades reguladoras sectoriais competentes;
j) servir de ponto de contacto 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;
k) definir o nível nacional de alerta e emitir instruções de segurança cibernética;
l) estabelecer códigos de conduta, padrões e normas na área de segurança cibernética alinhadas com as boas práticas internacionais.

Subsecção III

Equipa Nacional de Resposta a Incidentes de Segurança Cibernética

ARTIGO 12

(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 na resposta a 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.

ARTIGO13

(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) coordenar a Rede Nacional de CSIRTs;
c) servir de elo de ligação entre as redes nacionais de CSIRT e Autoridade Nacional de Segurança Cibernética;
d) supervisionar as equipas sectoriais de resposta a incidentes de Segurança Cibernética com particular incidência nos sectores das infra-estruturas críticas de informação;
e) garantir a partilha de informação sobre vulnerabilidades e incidentes de segurança cibernética com vista a prevenção e mitigação de crimes cibernéticos em Moçambique;
f) promover a adopção e a utilização de normas técnicas e práticas padronizadas; e
g) operacionalizar acções que visam estudos de pesquisa e análise de tráfego da Internet.

Subsecção IV

Entidades do Sistema Nacional de Segurança Cibernética

ARTIGO 14

(Rede Nacional de CSIRTs)

1. A Rede Nacional de CSIRTs é um fórum para partilha de informação de carácter operacional assegurando 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.
4. Os CSIRTs sectoriais partilham informação sobre incidentes cibernéticos e sua mitigação ao CSIRT Nacional.

Subsecção V

Operadores de Infra-estruturas Críticas

Artigo 15

(Natureza)

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

Artigo 16

(Competências)

1. Compete aos Operadores 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-estrutura crítica devem registar-se na Autoridade Nacional de Segurança Cibernética.

Subsecção VI

Provedores Intermediários de Serviços

ARTIGO 17

(Natureza)

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

Artigo 18

(Competências)

1. Compete aos Provedores Intermediários de Serviços:
   a) garantir o acesso e assegurar a comunicação de informação transmitida pelos utilizadores a ele vinculados, através de uma rede ou sistema de comunicação;
   b) implementar medidas de segurança cibernética que cumpram com padrões e normas de segurança cibernética nas suas infra-estruturas de TIC para proteger o sistema de segurança cibernética;
   c) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;
   d) fornecer 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 os Provedores Intermediários de Serviços devem registar-se na Autoridade Nacional de Segurança Cibernética.

Subsecção VII

Operadores de Serviços Essenciais

ARTIGO 19

(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 constam do anexo da presente Lei.
3. A actualização da lista dos serviços essenciais é feita pelo Conselho de Ministros

ARTIGO 20

(Competências)

1. Compete aos Operadores de Serviços Essenciais:
   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) comunicar de imediato a Autoridade Reguladora do Sector de TIC e ao CSIRT Nacional o exercício da respectiva actividade.

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

Subsecção VIII

Provedores de Serviços Digitais

ARTIGO 21

(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 22

(Competências)

1. Compete aos Provedores de Serviços Digitais:
   a) registar os utilizadores dos seus serviços;
   estabelecer o CSIRT institucional**;**
   b) adoptar medidas técnicas e organizacionais necessárias à antecipação, detecção, reacção e recuperação dos danos causados por incidentes 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;
2. Para o exercício das suas actividades os Provedores de Serviços Digitais devem registar-se na Autoridade Nacional de Segurança Cibernética.

Subsecção IX

Operadores de Plataformas Digitais

ARTIGO 23

(Natureza)

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 24

(Competências)

1. Compete aos Operadores de Plataformas Digitais:
   a) registar os utilizadores das suas plataformas;
   b) estabelecer o CSIRT institucional**;**
   c) adoptar medidas técnicas e organizacionais necessárias à antecipação, detecção, reacção e recuperação dos danos causados por incidentes cibernéticos;
   d) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados.
2. Para o exercício das suas actividades os Operadores de Plataformas Digitais devem registar-se na Autoridade Nacional de Segurança Cibernética.
3. Os Operadores de Operadores de Plataformas Digitais que prestam serviços ao Estado estão sujeitos a regulamentação específica.

Subsecção X

Operadores de Centros de Dados

ARTIGO 25

(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 dedicados ao alojamento, à interligação e à operação centralizadas de equipamento de redes de comunicação de dados e tecnologias da informação

ARTIGO 26

(Competências)

1. Compete aos Operadores 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 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) 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.

2. Para o exercício das suas actividades os Operadores de Centros de Dados devem registar-se na Autoridade Nacional de Segurança Cibernética.
3. Os Operadores de Centros de Dados que prestam serviços ao Estado estão sujeitos a regulamentação específica.

Subsecção XI

Operadores de Plataformas de Computação em Nuvem

ARTIGO 27

(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 28

(Competências)

1. Os Operadores de Plataformas de Computação em Nuvem têm as seguintes competências:
   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 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) 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 de Plataformas de Computação em Nuvem devem registar-se na Autoridade Nacional de Segurança Cibernética.
3. Os Operadores de Serviço de Computação em Nuvem Privada que prestam serviços ao Estado estão sujeitos a regulamentação específica.

Subsecção XII

Provedores de Serviços de Segurança Cibernética

ARTIGO 29

(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 30

(Competências)

1. Compete aos Prestadores de Serviços de Segurança Cibernética:
   a) comunicar de imediato a Autoridade Reguladora do Sector de TIC e ao CSIRT Nacional o exercício da respectiva actividade;
   b) descrever os serviços oferecidos e os processos técnicos envolvidos.
   c) manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;
   d) adoptar medidas técnicas e organizacionais necessárias à antecipação, detecção, reacção e recuperação dos danos causados por incidentes cibernéticos; e
   e) 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 os Prestadores de Segurança Cibernética devem registar-se na Autoridade Nacional de Segurança Cibernética.

Subsecção XIII

Operadores de Comunicações Digitais

ARTIGO 31

(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 32

(Competências)

1. Compete aos Operadores 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 os Operadores de Comunicações Digitais devem registar-se na Autoridade Nacional de Segurança Cibernética.

CAPÍTULO III

Segurança das Redes e dos Sistemas de Informação

SECÇÃO II

Segurança de Redes

ARTIGO 33

(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 privacidade das comunicações mediante a implementação de medidas de segurança lógica e física, estabelecidas no regime jurídico aplicável.

ARTIGO 34

(Segurança da Internet)

1. Compete aos Provedores de Serviços de Internet (ISP) assegurar a confidencialidade, integridade, disponibilidade e privacidade dos dados e da informação mediante a implementação de medidas de segurança lógica e física, estabelecidas no regime jurídico aplicável.
2. Sem prejuízo dos termos e condições aplicáveis para utilização do espaço cibernético, os Provedores de Serviços de Internet devem registar os seus utilizadores e aplicar medidas necessárias à antecipação, detecção, reacção e recuperação dos danos causados por incidentes cibernéticos.

ARTIGO 35

(Protecção do Sistema de Nomes de Domínio)

1. Compete a Autoridade Reguladora de Tecnologias de Informação e Comunicação garantir a segurança do Sistema de Nomes de Domínio (DNS) através da utilização de Extensões de Segurança do Sistema de Nomes de Domínio (DNSSEC), esquema de criptografia que faz uso de chaves públicas e privadas para garantir a autenticidade dos endereços consultados e sua tradução para o número de IP correcto, evitando ataques do DNS e fraudes na Internet.

2. A Segurança do Sistema de Nomes de Domínio, nos termos a regulamentar.

ARTIGO 36

(Resposta a Incidentes nas Redes do Espaço Cibernético)

1. Compete ao CSIRT Nacional estabelecer as medidas técnicas e operacionais de resposta aos ataques, roubos, furtos e quaisquer outros incidentes cibernéticos.

2. Os Reguladores sectoriais e os Governos Provinciais devem estabelecer CSIRTs Sectoriais e garantir a criação de CSIRTs institucionais.

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

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 confidencialidade, segurança de dados de tráfego e de localização e ordenar a conservação expedita de dados.

2. Os dados referidos no número anterior devem ser preservados por um período mínimo de 2 anos.

ARTIGO 38

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

O provedor intermediário de serviços no espaço cibernético ou o provedor 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 deve indicar as outras entidades que nela participam, permitindo a identificação das mesmas, nos termos a regulamentar.

ARTIGO 39

(Preservação de provas)

1. O Provedor Intermediário de Serviços e o Provedor de Serviços Digitais que tenha armazenado num determinado Sistema de Informação, dados de tráfego e de localização necessários a 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 anterior devem ser conservados por um período mínimo de 1 ano, contados a partir da data da conclusão da comunicação.
3. O período de preservação de provas definido no número anterior 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 anterior 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 III

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 garantam 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 XVII

Programas de Computador e Bases de Dados

ARTIGO 45

(Programas de computador)

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

ARTIGO 46
(Bases de dados)

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

CAPÍTULO IV

Requisitos de Segurança e Notificação de Incidentes

SECÇÃO IV
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

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

1. Constituem entidades sujeitas aos requisitos de notificação as seguintes:
   a) Administração Pública;
   b) Operadores de Infra-estruturas Críticas;
   c) Provedores Intermediários de Serviços;
   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.

3. Os requisitos de notificação de incidentes não se aplicam:

   a) às redes e sistemas de informação directamente relacionados com o comando e controlo das FDS;

   b) às redes e sistemas de informação que processam informação classificada conforme a regulamentação específica.

ARTIGO 49

(Requisitos de segurança para a Administração Pública)

1. As entidades da Administração Pública devem cumprir com 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 anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.
3. As entidades da Administração Pública devem tomar as medidas adequadas previstas na presente Lei e em regulamento específico para prevenir e mitigar os incidentes cibernéticos que afectam a segurança das redes e dos sistemas de informação utilizados e para reduzir o seu impacto.
4. O responsável pela área administrativa das entidades da Administração Pública deve nomear o responsável e o auditor interno da segurança cibernética para melhor gestão de riscos cibernéticos.
5. As entidades da Administração Pública devem estabelecer um CSIRT institucional.

ARTIGO 50

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

1. Os Operadores de Infra-estruturas Críticas 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 anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.
3. Os Operadores de Infra-estruturas Críticas devem tomar as medidas adequadas para evitar os incidentes que afectam a segurança das redes e dos sistemas de informação utilizados e para reduzir seu impacto.

ARTIGO 51

(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 anterior 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 52

(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) 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
    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 53

(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 anterior, 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 a 3 do presente artigo são estabelecidas nos termos a regulamentar.

ARTIGO 54

(Requisitos de segurança para Operadores de Centros de Dados)

1. Um operador de Centro de Dados é uma entidade dedicada ao arranjo, processamento, armazenamento e distribuição 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 55

(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 V

Notificação de Incidentes de segurança cibernética

ARTIGO 56

(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 57

(Notificação de incidentes para a Administração Pública)

1. As entidades da Administração Pública 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 deve acarretar 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 sectorial 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 relativo as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 58

(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 permita ao CSIRT sectorial e ao CSIRT Nacional determinar o impacto dos incidentes.

3. A notificação não deve acarretar 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 59

(Notificação de incidentes para os Operadores de Serviços Essenciais)

1. Os Operadores de Serviços Essenciais notificam 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 permita à Autoridade Nacional de Segurança Cibernética determinar o impacto dos incidentes.
3. A notificação não deve acarretar 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

   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 CSIRTs;

   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 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 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 anterior inclui informação que permita 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 informações 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 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 anterior inclui informação que permita 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

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

5. A obrigação de notificar um incidente só se aplica se os Provedores Intermediários de Serviços Digitais que tiver acesso à informação necessária para avaliar o impacto de um incidente em função dos factores a que se refere o n.º 2 do artigo 60.

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

7. 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.

8. O relatório da resposta e da 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 62

(Notificação de incidentes para Operadores de Centros de Dados)

1. Os Operadores de Centros de Dados 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;

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

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 informações 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 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

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 informações sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas e o respectivo impacto.

ARTIGO 64

(Notificação voluntária de incidentes)

1. Sem prejuízo da obrigação de notificação de incidentes prevista na presente Lei, quaisquer entidades podem notificar ao 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 as disposições relativas a 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 65

(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 informações e não tiver sido solicitada a recompensa;

    b) ter sido dado um prazo razoável de pelo menos 90 dias do calendário, para corrigir a vulnerabilidade antes de publicá-la ou divulgá-la;

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

    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 de 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.

4. A divulgação responsável de vulnerabilidade não se aplica às redes e sistemas de informação e comunicação relacionados com o comando e controlo das Força de Defesa Armada.

CAPÍTULO VI

Fundo de Segurança Cibernética

ARTIGO 66

(Fundo)

1. É instituído pela presente Lei um Fundo de Segurança Cibernética (FSC) com o objectivo de fornecer 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 devem contribuir para o FSC.
4. As regras de funcionamento do FSC são estabelecidas em regulamentação específica.

ARTIGO 67

(Objectivos)

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 68

(Beneficiários)

São beneficiários do FNSC**:**

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 contribuintes do FNSC, 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 contribuintes 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 69

(Fontes de receitas)

1. Constituem fontes de receitas do FNSC:

a) as comparticipações e subvenções, que sejam atribuídas pelo Estado e por outras pessoas colectivas do direito público;
b) as contribuições dos parceiros de cooperação destinadas ao financiamento da área de segurança cibernética;
c) as Entidades do Sistema Nacional de Segurança Cibernética, licenciadas no âmbito do exercício da actividade de prestação de serviços de segurança cibernética contribuem para o fundo até 1% da receita bruta do ano anterior;
d) outras fontes de receitas ou financiamento que lhe vierem a ser destinados.

Artigo 70

(Gestão)

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

CAPÍTULO VI

Supervisão, Fiscalização, Contravenções e Sanções

Artigo 71

(Supervisão)

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

Artigo 72

(Fiscalização)

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

Artigo 73

(Auditoria)

1. 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 74
(Contravenções)

1. Constituem contravenções à presente Lei:
    a) a violação da responsabilidade do responsável de uma infra-estrutura de informação crítica registada de informar a Autoridade Nacional de Segurança Cibernética no prazo de 7 dias a contar da mudança de propriedade legal da infra-estrutura de informação crítica registada;
    b) a falha do responsável de uma infra-estrutura de informação crítica 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 de informação crítica em apresentar uma cópia do relatório de auditoria à Autoridade de Segurança Cibernética;
    e) o incumprimento das directrizes regulatórias de uma Equipa de Resposta a Incidentes de Segurança Computacionais emanada pela Autoridade Nacional de Segurança Cibernética;

f) a recusa do responsável de uma 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 de padrões de segurança cibernética;
j) a má utilização do Provedor de Serviços em instalar um recurso de interceptação para executar um mandado de interceptação emitido por um tribunal de jurisdição competente;
k) a violação da responsabilidade do Provedor de Serviços em adoptar medidas necessárias para desencriptar uma mensagem de telecomunicação de acordo com um mandado de interceptação;
l) a recusa do Provedor de Serviço em não reter informações de assinante por um período de 1 ano;
m) a recusa do Provedor de Serviços em não reter dados de tráfego por um período de 1 ano;
n) a violação da responsabilidade do Provedor de Serviços em não reter dados de tráfego por um período de 1 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, uma Equipa Sectorial de Resposta a Emergências Informáticas designada ou um Provedor de Serviço Digital em apresentar informações relevantes à Autoridade;
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 ameace ou afecte a segurança cibernética do país;
r) o incumprimento de uma directiva emanada pela Autoridade Nacional de Segurança Cibernética;
s) Incumprimento diário por parte do responsável de uma infra-estrutura de informação crítica, de uma Equipa Sectorial de Resposta a Emergências Informática designada ou de um prestador de serviço digital em cumprir um pedido de envio de informação relevante com a finalidade de garantir a segurança cibernética do país;
t) o incumprimento da obrigação de requisitos de segurança previsto nos artigos 49, 50, 51, 52, 53, 54, 55;
u) o incumprimento da obrigação de notificação de incidentes de segurança previsto nos artigos 57, 58, 59, 60, 61, 62, 63, 64, 65;
v) o incumprimento das instruções e alertas de segurança cibernética emitidas pela Autoridade Nacional de Segurança Cibernética previsto na alínea g) do artigo 11;
w) todos os factos ilícitos que preencham um tipo legal correspondente á violação de disposições legais relativas a segurança cibernética para as quais caiba

multa, suspensão de licenças, certificados, autorizações ou proibição de operação ou sanção estabelecidas em legislação específica.

Artigo 75

(Sanções)

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

a) a violação do disposto na alínea h) do artigo 74 é punível com a multa de 35 salários mínimos da função pública;
b) a violação do disposto da na alínea q) do artigo 74 é punível com a multa de 2 salários mínimos até ao valor máximo de 17 salários mínimos da função pública;
c) a violação do disposto nas alíneas j) e k) do artigo 74 é punível com a multa de 7 salários mínimos da função pública;
d) a violação do disposto nas alíneas a), b), c), d), l), m), n), o), p) e s) do artigo 74 é punível com a multa de 1 salário mínimo até ao valor máximo de 7 salários mínimos da função pública;
e) a violação do disposto nas alíneas e), f) e i) do artigo 74 é punível com a multa de 1 salário mínimo até ao valor máximo de 4 salários mínimos da função pública;
f) a violação do disposto nas alíneas r) e t) do artigo 74 é punível com a multa de 1 salário mínimo da função pública por semana;
g) a violação do disposto na alínea g) do artigo 74 é punível com a multa de 64 salários mínimos da função pública;
h) a violação da obrigação de requisitos de segurança previsto nos artigos 46, 48, 50, 52, 54, 56 e 58 é punível com uma multa de 90 salários mínimos até ao valor máximo de 160 salários mínimos da Função Pública;
i) a violação da obrigação de notificação de incidentes de segurança previsto nos artigos ,47, 49, 51, 53, 55, 57 e 59, é punível com a multa de 80 salários mínimos até ao valor máximo de 100 salários mínimos da Função Pública, a violação da observância das instruções e alertas de segurança cibernética emitidas pela Autoridade Nacional de Segurança Cibernética tal como previsto na alínea g) do artigo 11 é punível com a multa de 60 salários mínimos até ao valor máximo de 90 salários mínimos da Função Pública.

Artigo 76

(Receitas)

1. Constituem receitas:
   a) as dotações provenientes do orçamento do Estado;
   b) as taxas de licenciamento de Provedores de Serviços de Segurança Cibernética;
   c) comparticipações e subvenções que sejam atribuídas pelo Estado e outras pessoas colectivas do direito público;
   d) as multas no âmbito da fiscalização dos serviços nos termos da legislação aplicada;
   e) quaisquer outros rendimentos ou valores que provenham da sua actividade ou por contracto que venham a perecer.

2. As receitas próprias revertem-se em:
   a) 20 % para o Estado;
   b) 80 % para à Autoridade Reguladora.

CAPÍTULO VII

Disposições finais

Artigo 77

(Regime subsidiário)

É aplicável subsidiariamente a presente Lei, em tudo que se mostre omissa, o regime jurídico aplicável às transacções electrónicas e demais legislações complementares.

Artigo 78

(**Regulamentação**)

Compete ao Governo Regulamentar a presente Lei no prazo de 90 dias a contar da data da sua publicação no Boletim da República.

Artigo 79

(Entrada em vigor)

A presente Lei entra em vigor na data da sua publicação.

Aprovada pela Assembleia da República, aos….. de …… de 2023

A Presidente da Assembleia da República, *Esperança Laurinda Francisco Nhiuane Bias*

Promulgada aos …de de 2023

Publique se.

O Presidente da República, Filipe Jacinto Nyusi

ANEXO I

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	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias.

#	Sector	Subsector	Tipo de Entidade
		interiores	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.
		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	Infraestruturas 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	Infraestruturas de Telecomunicações	--	Operadoras de Telecomunicações
8	Infraestruturas 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

ANEXO II

Glossário

Para efeitos do presente regulamento, entende-se por:

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 a 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 disponibilidades de dados e informações numa organização

E

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

Equipa de resposta a incidentes de segurança cibernética - 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;

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;

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.

R

Rede e sistema de informação - qualquer ou 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 - refere-se ao Estado e ao conjunto de práticas destinado a mantê-lo, no qual um activo, sistema de informação ou serviço de tecnologia da informação e comunicação atende às seguintes condições: Se estiver protegido contra acesso não autorizado; Se permanecer disponível e operacional; Se a integridade do activo, sistema ou serviço for mantida; Se a integridade e confidencialidade das informações forem mantidas armazenados, processados ou transmitidos através do sistema de informação.

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 todo o dispositivo ou conjunto de dispositivos que usam tecnologias de informação e comunicação, bem como qualquer sistema de alta tecnologia e tecnologias emergentes, incluindo sistemas electrónicos, de computador, telemáticos e de comunicação. telecomunicações que, isolada ou conjuntamente, servem para gerar, enviar, receber, arquivar ou processar informações, documentos digitais, mensagens de dados, entre outros.

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 - é 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.