REPÚBLICA DE ANGOLA

PROPOSTA DE LEI DA CIBERSEGURANÇA

PROPONENTE: MINISTÉRIO DAS TELECOMUNICAÇÕES, TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO SOCIAL

Luanda, Fevereiro de 2025

ÍNDICE

RELATÓRIO FUNDAMENTAÇÃO

I. ENQUDRAMENTO DA PROPOSTA DE LEI

1.1. Na era da transição digital em que vivemos, a defesa do ciberespaço tem sido conduzida predominantemente através de políticas de curto e médio prazo, dado que estas oferecem maior flexibilidade em comparação com a legislação. O processo de alteração legislativa, por sua natureza burocrática, muitas vezes não acompanha a urgência das respostas necessárias diante de ciberameaças ou ciberataques.

1.2. De facto, apesar dos esforços institucionais, políticos e legais empreendidos nos últimos anos no domínio da segurança cibernética em Angola, o Índice Global de Cibersegurança de 2024, elaborado pela União Internacional de Telecomunicações (UIT), agência especializada das Nações Unidas para as tecnologias de informação e comunicação, classifica Angola na quarta posição a partir do nível mais baixo, com uma pontuação de 39,5 em uma escala de 100.

1.3. Dentre outros aspectos, a inexistência de uma estratégia nacional para este sector e a falta de órgãos especializados habilitados a assegurar a segurança do ciberespaço nacional, como é o caso do

Conselho Nacional de Cibersegurança e do Centro Nacional de Cibersegurança, são algumas das razões da obtenção da pontuação supracitada.

1.4. Por isso, para além da melhoria das normas sobre a segurança das redes e sistemas informáticos, a presente Proposta enfatiza a indispensabilidade de se institucionalizar os mecanismos institucionais e estratégicos acima citados, de modo a garantir o normal funcionamento das instituições públicas e privadas, sem olvidar da necessidade de respeitar os direitos, liberdades e garantias individuais, por via de um sistema eficiente de protecção de dados pessoais.

1.5. A presente Proposta de Lei procura, ainda, garantir que Angola tenha uma posição desejável no Índice Global de Cibersegurança, se apresentando como um Estado que adere aos padrões internacionais de regulação da segurança cibernética, alinhando-se aos outros países, promovendo a cooperação global e assegurando a competitividade tecnológica no mercado internacional.

II. ENQUADRAMENTO JURÍDICO-LEGAL E NO PLANO DA GOVERNAÇÃO

2.1. A matéria objecto do presente diploma encontra-se consagrada nos artigos 11.º, 202.º e 203.º da Constituição da República de Angola, que prevê a defesa da segurança nacional, abrangendo a protecção das infra-estruturas críticas e dos sistemas informáticos.

2.2. Do ponto de vista da governação, a presente proposta de lei encontra-se reflectida no Plano de Desenvolvimento Nacional 2022-2027, que prevê criar capacidade do Estado no domínio da cibersegurança, através de três acções principais, nomeadamente:

a) Implementação de um plano operacional de cibersegurança e dotá-lo dos meios orçamentais indispensáveis à sua implementação;
b) Estruturação das unidades operacionais de cibersegurança, capacitando os efectivos das mesmas;
c) Melhoria do suporte tecnológico, adequando-o aos desafios e ameaças que enfrentamos.

2.3. Adicionalmente, a proposta de Lei que agora se apresenta enquadra-se no Livro Branco das Tecnologias de Informação e Comunicação, que prevê, por um lado, criar um quadro legislativo sectorial que permita legislar sobre as novas áreas que suscitam desafios a um Sector das Tecnologias de Informação e Comunicação integrado e abrangente a todos os sectores da economia nacional e em conformidade com a Constituição da República de Angola.

2.3.1. Outrossim, a proposta está alinhada a visão do Executivo vertida no instrumento supracitado, na medida em que prevê como um dos principais objectivos que o Estado Angolano pretende alcançar no domínio da cibersegurança afirmar o País no contexto internacional, melhorando os seus indicadores internacionais no domínio das Tecnologias de Informação e Comunicação.

III. RAZÕES QUE JUSTIFICAM A ELABORAÇÃO DA PROPOSTA DE LEI

3.1. No contexto actual, o sector das telecomunicações e das Tecnologias de Informação está em constante evolução, fruto da convergência tecnológica e de serviços, tornando-se imperativo que o quadro jurídico-legal vigente acompanhe e acomode essa evolução, assegurando uma maior eficiência do mercado das comunicações electrónicas. Com efeito, faz-se necessário e indispensável que, de forma periódica, se avalie a adequação da legislação em vigor à nova realidade do mercado.

3.2. Na verdade, a Lei n.º 7/17, de 16 de Fevereiro, sobre a Protecção das Redes e Sistemas Informáticos, é um marco no quadro da cibersegurança, uma vez que está focada na protecção do espaço cibernético de Angola contra os riscos associados.

3.3. No entanto, a crescente dinâmica e a busca de uma maior garantia de segurança do mercado digital, tornou-se um desafio crucial devido ao aumento das ameaças cibernéticas e da pouca clareza da legislação em vigor, urgindo a necessidade da sua revisão e actualização.

3.4. A revisão à Lei sobre Protecção das Redes e Sistemas Informáticos e consequente aprovação da Lei da Cibersegurança é uma resposta ao ambiente de ameaças em constante mudança e às crescentes expectativas sociais em relação à segurança dos serviços digitais.

3.5. As mudanças visam fortalecer a resiliência de sectores-chave da economia, melhorar a coordenação de actividades e troca de

informações e aumentar o potencial do País para prevenir e responder a incidentes.

3.6. A implementação dos comandos da nova legislação exigirá um esforço significativo por parte de todos os integrantes do Sistema Nacional da Cibersegurança – desde a administração pública, passando pelos operadores de serviços essenciais, até os fornecedores de soluções de segurança cibernética.

3.7. Será crucial disponibilizar recursos, competências e ferramentas adequados para a realização de novas tarefas, bem como uma cooperação e comunicação eficazes entre todas as partes interessadas.

3.8. O teste final da eficácia da legislação proposta será a prática da sua aplicação em face das ameaças e incidentes reais. Somente por meio da melhoria contínua e da adaptação às mudanças que se impõem, o Sistema Nacional de Segurança Cibersegurança será capaz de proteger efetivamente o ciberespaço angolano e apoiar o desenvolvimento seguro da economia digital.

IV. OBJECTIVOS DA PROPOSTA

4.1. Em articulação com o Livro Branco das Tecnologias de Informação e Comunicação, aprovado por Decreto Presidencial n.º……., bem como com o Plano de Desenvolvimento Nacional, PDN - 2023-2027, aprovado por Decreto Presidencial nº 225/23 de 30 de Novembro, a presente Proposta assegura a criação da capacidade do

Estado Angolano em matéria de cibersegurança, por intermédio da implementação de um plano operacional de ciberdefesa e dotá-lo dos meios orçamentais indispensáveis à sua implementação, bem como através da estruturação das unidades operacionais de ciberdefesa, capacitando os efectivos das mesmas e da melhoria do suporte tecnológico, adequando-o aos desafios e ameaças que enfrentamos.

4.2. Com a presente Proposta de alteração da Lei de Protecção das Redes e Sistemas Informáticos pretende-se tornar Angola numa Nação segura e resiliente do ponto de vista cibernético, em que a preocupação com a segurança cibernética se apresenta como o mote da garantia dos valores mais estruturantes do Estado Democrático e de Direito consagrados na Constituição, sem prejuízo da necessidade de preservação dos dados pessoais dos cidadãos.

4.3. Outrossim, a presente Proposta visa criar e desenvolver uma capacidade legal, institucional e operacional que garanta um ambiente seguro e atractivo no ciberespaço nacional, garantindo um espaço cibernético seguro, que fomenta uma cultura de cibersegurança responsável entre os cidadãos e as instituições públicas e privadas.

4.4. Em suma, a Proposta de Lei de alteração da Lei de Protecção de Redes e Sistemas Informáticos pretende:

a) Criar um quadro jurídico-legal e técnico-operacional alinhado aos desafios actuais da segurança cibernética;
b) Aumentar a resiliência institucional, operacional e jurídico-legal do Estado Angolano face a ciberameaças, ciberataques e cibercriminalidade;

c) Fortalecer a actuação de Angola em cibersegurança no contexto regional e internacional;
d) Criar um quadro institucional forte para Angola, com a institucionalização de entidades especializadas em matéria de segurança cibernética.

V. IMPACTO SOCIOECONÓMICO DA PROPOSTA DE LEI

Em termos económicos, a capacidade institucional, operacional e estratégica que se pretende criar com a Presente Lei produz impacto imediato e directo no Orçamento Geral do Estado.

VI. ÓRGÃOS CONSULTADOS

6.1. A elaboração da presente proposta de Lei foi submetida à consulta pública em que participaram todas as entidades, públicas e privadas, bem como as individualidades interessadas nas matérias de segurança cibernética.

6.2. Da referida consulta pública participaram, nomeadamente, as seguintes entidades, que remeteram as suas contribuições escritas:

a) ……..;
b) ……..;

VII. ANÁLISE COMPARATIVA ENTRE O REGIME JURÍDICO EM VIGOR E O REGIME JURÍDICO A APROVAR

7.1. A Lei de Protecção de Redes e Sistemas Informáticos carece de algumas melhorias face a dinâmica que o actual contexto nacional e internacional da cibersegurança impõe. Esta necessidade de actualização decorre do facto de este Diploma apresentar debilidades no que a prevenção e combate eficiente da cibercriminalidade dizem respeito, tais como, por exemplo, as seguintes:

a) Não estabelecimento de um mecanismo claro para monitorar o cumprimento das medidas nela prevista e aplicar as penalidades em caso de não conformidade dos operadores das redes e sistemas informáticos;

b) Falha na definição clara de requisitos e medidas de segurança que devem ser adoptadas no âmbito da protecção das infra-estruturas críticas e serviços essenciais;

c) Falta de previsão clara de uma estrutura institucional capaz de avaliar e monitorar, de modo contínuo, o cumprimento dos requisitos e medidas de segurança nela prevista;

d) Apresentar debilidades no que diz respeito à garantia institucional do Ciberespaço, uma vez que não trata, de forma criteriosa e desenvolvida, sobre o Sistema Nacional da Cibersegurança;

e) Falta de previsão da possibilidade de aprovação da Estratégia Nacional de Cibersegurança.

7.2. Daí que a Lei da Cibersegurança que se propõe, para além de estar alinhada aos padrões universais de segurança cibernética, introduz uma série de alterações significativas destinadas a reforçar a resiliência do ciberespaço angolano e a adaptar o quadro jurídico nacional aos novos desafios e às normas internacionais.

7.3. A propósito, a proposta de Lei impõe o cumprimento rigoroso de determinados requisitos de segurança e também a obrigação de notificação de determinados incidentes com impacto relevante nas redes e sistemas de informação das entidades da Administração Pública, dos operadores de infra-estruturas críticas, dos operadores de serviços essenciais, bem como dos prestadores de serviços digitais.

7.4. Em suma, a Lei da Cibersegurança ora proposta prevê as seguintes mudanças:

a) Extensão do âmbito da Lei, que estabelece um sistema nacional, define as entidades responsáveis pelo sistema, expande o catálogo de entidades cobertas para incluir outros sectores, como infra-estrutura digital, plataformas de comércio eletrônico e serviços de confiança, o que significa que mais empresas terão que implementar os requisitos da Lei e cooperar com as autoridades do Sistema Nacional de Cibersegurança;

b) Reforço dos requisitos aplicáveis aos operadores de serviços, com a introdução de medidas de segurança mais pormenorizadas e restritivas para a gestão dos riscos, a notificação de incidentes e a aplicação de medidas de segurança. Neste aspecto, as operadoras são obrigadas a realizar auditorias regulares de segurança e testes de penetração dos seus sistemas, entre outros;

c) Criação do Conselho Nacional de Cibersegurança, órgão de consulta do Titular do Poder Executivo em matéria de segurança cibernética, que deverá, dentre outras tarefas, assegurar a coordenação político-estratégica para a segurança cibernética em Angola;

d) Criação da Estratégia Nacional de Cibersegurança, com vista a maximização da resiliência do País no combate a cibercriminalidade, da promoção da inovação tecnológica e do asseguramento de recursos financeiros para o Estado, através de investimento privado estrangeiro;

e) Estabelecimento de CERT. Nacional, CERTs sectoriais e institucionais, dedicadas ao asseguramento do nível de respostas a incidentes informáticos, os sectores e as instituições individuais da economia, que apoiarão os operadores de serviços-chave na implementação de requisitos de segurança cibernética e na resposta a incidentes informáticos;

f) Estabelecimento do Fundo de Segurança Cibernética, que assegurará a implementação de projectos que fortaleçam as capacidades nacionais de cibersegurança, como pesquisa, treinamento e investimentos em infra-estrutura;

g) Reforço da cooperação internacional, com a previsão de mecanismos mais eficientes para o intercâmbio de informações sobre ameaças e a participação de Angola no contexto internacional e regional da cibersegurança;

h) Maior transparência e controle, com a introdução de novas obrigações de emissão de relatórios de actividades dos órgãos do Sistema Nacional Cibersegurança.

VIII. SUMÁRIO A PUBLICAR NO DIÁRIO DA REPÚBLICA

8.1. Eis o sumário que deve constar da Iª Série do Diário da República:

"Lei n.º ___/2024, Lei da Cibersegurança."

IX. CONFORMAÇÃO LEGAL

9.1. A presente proposta de Lei e respectivo relatório de fundamentação estão em conformidade e harmonizados com o disposto na Lei n.º 7/14, de 26 de Maio, sobre as Publicações Oficiais e Formulários Legais, com o Regimento da Assembleia Nacional, aprovado pela Lei n.º 13/17, de 6 de Julho, com o Decreto Presidencial n.º 251/12, de 27 de Dezembro, que estabelece os Procedimentos para Materialização das Deliberações do Executivo e com o Regimento do Conselho de Ministros, aprovado pelo Decreto Presidencial n.º 357/17, de 28 de Dezembro.

X. FORMA PROPOSTA PARA O DIPLOMA

10.1. A presente proposta de Lei reveste a forma de Lei, ao abrigo das disposições combinadas da alínea b) do artigo 161.º, n.º 2 do artigo 165.º e da alínea d) do n.º 1 do artigo 166.º da Constituição da República de Angola (CRA).

XI. LEGISLAÇÃO A REVOGAR

11.1. É revogada a Lei n.º 7/17, de 16 de Fevereiro, Lei de Protecção de Redes e Sistemas Informáticos.

XII. NOTA PARA A COMUNICAÇÃO SOCIAL

12.1. Recomenda-se, para os órgãos de comunicação social, a seguinte nota de imprensa:

- *"O Conselho de Ministros apreciou hoje a Proposta de Lei da Cibersegurança e recomendou a sua remessa para a Assembleia Nacional. A proposta de Lei apreciada irá revogar a Lei n.º 7/17, de 16 de Fevereiro, Lei de Protecção de Redes e Sistemas Informáticos, visando ajustar quadro normativo aplicável à cibersegurança à rápida evolução verificada n*o sector das telecomunicações e das tecnologias de informação, que aconselha o reforço das medidas para enfrentar as ameaças e os riscos, quer no plano político-legal, quer no plano operacional."

XIII. SÍNTESE DO CONTEÚDO DA PROPOSTA DE LEI

13.1. De forma geral, ao contrário da Lei actualmente em vigor, a presente Proposta conta com 72 artigos e sete capítulos, contendo normas respeitantes ao regime jurídico-legal da cibersegurança em Angola, nomeadamente:

CAPÍTULO I: DISPOSIÇÕES GERAIS

Artigo 1.º Objecto
Artigo 2º Âmbito
Artigo 3. º Regime Jurídico subsidiário
Artigo 4º Definições
Artigo 5.º Cooperação internacional
Artigo 6.º Estratégia Nacional de Cibersegurança

CAPÍTULO II: ORGANIZAÇÃO DO SISTEMA NACIONAL DA CIBERSEGURANÇA

Secção I: Disposições Gerais
Artigo 7.º Estruturas do Sistema de Segurança do Ciberespaço

Secção II: Conselho Nacional de Cibersegurança
Artigo 8.º Natureza
Artigo 9.º Estrutura, organização e funcionamento

Secção III: Centro Nacional de Cibersegurança
Artigo 10.º Natureza
Artigo 11.º Estrutura, organização e funcionamento

Secção IV: Rede Nacional de CSIRTs
Artigo 12.º Natureza

Secção V: Operadores de Infra-estruturas Críticas e Serviços Essenciais

Subsecção I: Operadores de Infra-estruturas Críticas
Artigo 13.º Natureza
Artigo 14.º Obrigações dos Operadores de Infra-estruturas Críticas

Subsecção II: Operadores de Serviços Essenciais

PROPOSTA DE LEI DA CIBERSEGURANÇA

Lei n. _____/2024

de _____de _____

Considerando que o sector das Telecomunicações e das Tecnologias de Informação está em constante evolução, fruto da convergência tecnológica e de serviços, tornando-se imperativo que o quadro jurídico-legal vigente acompanhe e acomode essa evolução, assegurando uma maior eficiência do mercado das comunicações electrónicas;

Considerando, ainda, que a Lei de Protecção de Redes e Sistemas Informáticos, Lei n.º 7/17 de 16 de Fevereiro, carece de alterações profundas e estruturantes face aos desafios actuais que se colocam no domínio da segurança cibernética, visando a protecção eficaz das redes, dos sistemas de informação, das infra-estruturas críticas e dos serviços essenciais para os cidadãos e instituições públicas e privadas;

A Assembleia Nacional aprova, por mandato do povo, nos termos da alínea b) do artigo 161.º, n.º 2 do artigo 165.º e da alínea d) do n.º 1 do artigo 166.º, todos da Constituição da República de Angola, a seguinte:

LEI DA CIBERSEGURANÇA

CAPÍTULO I
DISPOSIÇÕES GERAIS

ARTIGO 1.º
(Objecto)

A presente Lei estabelece o regime jurídico da cibersegurança e visa garantir a segurança do cidadão e instituições públicas e privadas, bem como assegurar a protecção de redes, sistemas de informação e infra-estruturas críticas do País.

ARTIGO 2º
(Âmbito)

1. A presente Lei aplica-se à rede de qualquer pessoa singular, colectiva pública ou privada, nos domínios dos provedores de serviços digitais, nomeadamente:
   a) À Administração Pública;
   b) Aos operadores de infra-estruturas críticas;
   c) Aos operadores de serviços essenciais;
   d) Aos provedores de serviços digitais;
   e) Aos operadores de plataformas digitais;
   f) A quaisquer outras entidades que utilizam redes de comunicação de dados e sistemas de informação.

2. A presente Lei aplica-se aos prestadores de serviços digitais que tenham o seu estabelecimento principal em território nacional ou, não o tendo, designem um representante estabelecido em território nacional, desde que aí prestem serviços digitais.

3. Para efeitos do número anterior, considera-se que um prestador de serviços digitais tem o seu estabelecimento principal em território nacional quando aí tiver a sua sede.

4. Caso uma entidade se enquadre simultaneamente em mais do que uma das alíneas a) a c) do n.º 1, aplica-se o regime que resultar mais exigente para a segurança das redes e dos sistemas de informação.

5. Sem prejuízo do disposto no número 1 do presente artigo, a presente lei aplica-se:
    a) Às redes e sistemas de informação directamente relacionados com o comando e controlo das entidades que superintendem as áreas da Defesa e Segurança Nacional e da Ordem e Segurança Pública;
    b) Às redes e sistemas de informação que processem informação classificada conforme a legislação específica.

6. A presente Lei aplica-se, igualmente, sem prejuízo do disposto no Código Penal, aos factos:
    a) Cometidos em território nacional por cidadãos angolanos, estrangeiros ou por pessoa colectiva com domicílio em território angolano, que visem o ciberespaço ou dados informáticos;
    b) Praticados fisicamente, total ou parcialmente, em território angolano, ainda que visem sistemas de informação ou dados localizados fora desse território;
    c) Praticados no ciberespaço ou dados localizados em território angolano, independentemente do local onde esses factos forem fisicamente praticados;
    d) Cometidos por cidadãos estrangeiros não residentes em território angolano, que visem o ciberespaço ou dados informáticos.

7. O disposto na presente Lei não prejudica o cumprimento da legislação aplicável em matéria dos ~~os~~ Tratados e das Convenções Internacionais, continentais e regionais vigentes na ordem jurídica nacional.

ARTIGO 3. º

(Regime Jurídico subsidiário)

Constitui regime jurídico subsidiário a presente lei:

e) O disposto nas normas constantes dos Tratados e das Convenções Internacionais, continentais e regionais vigentes na ordem jurídica nacional em matéria de cibersegurança;

f) O disposto em legislação vigente que seja compatível com a presente Lei, nomeadamente:

i) O regime jurídico de protecção de dados pessoais;

ii) O regime jurídico das tecnologias e dos serviços da sociedade da informação;

iii) O regime jurídico das comunicações electrónicas e dos serviços da sociedade da informação.

ARTIGO 4.º

(Definições)

Para efeitos da presente Lei, considera-se:

a) «Acesso condicional» – A sujeição do acesso de um serviço a uma assinatura ou qualquer outra forma de autorização prévia individual;

b) «Assinante» – A pessoa singular ou colectiva que é parte num contrato com um operador de comunicações electrónicas acessíveis ao público;

c) «Base de dados» – As colectâneas de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros;

d) «CERT.ao» – que corresponde ao Departamento da Equipa de Resposta a Emergências Informáticas, é o serviço executivo do Contro Nacional de Cibersegurança responsável pela coordenação e execução das actividades operacionais relacionadas com a prevenção, detecção, resposta e mitigação de incidentes cibernéticos.

e) «Ciberataque» – O ataque efectuado geralmente através da Internet, no qual são violados sistemas informáticos, com o objectivo de espiar, provocar danos, roubar dados;

f) «Ciberespaço» – O conjunto dos sistemas tecnológicos e infra-estruturas de redes telemáticas, bem como do conjunto de informações e serviços da Internet;

g) «Cibercrime» – O crime cometido com o recurso aos sistemas electrónicos e as novas tecnologias de informação e comunicação;

h) «Cibersegurança› – A segurança relacionada com o ciberespaço;

i) «Código de acesso» – Dado ou senha que permite aceder, no todo ou em parte e sob forma inteligível, à um sistema de informação;

j) «Código de identificação do utilizador (User ID)» – O código único atribuído às pessoas, quando estas se tomam assinantes ou se registam num serviço de acesso à *internet,* ou num serviço de comunicação pela *internet;*

k) «Conteúdo discriminatório» – Qualquer palavra, imagem ou outro que defenda, promova ou incite ao ódio ou a actos de violência contra uma pessoa ou grupo de pessoas por causa da sua raça, origem étnica, cor, nacionalidade, religião ou orientação sexual, com o propósito de os discriminar;

l) «Dados» – Qualquer representação de factos, vídeos ou imagens, informações ou conceitos, incluindo de programas de computador, que são armazenados, transmitidos ou processados num sistema de informação;

m) «Dados de base pessoais» – Os dados que permitem identificar uma pessoa, como seja o nome, idade, morada, telefone e endereço de correio electrónico;

n) «Dados de localização» – Quaisquer dados tratados num sistema de informação que indiquem a posição geográfica do equipamento terminal ou de um utilizador de um serviço prestado através de um sistema de informação;

o) «Dados de tráfego» – Qualquer dado tratado para efeitos do envio de uma comunicação, através de um sistema de informação ou para efeitos de facturação daquela, incluindo os dados que indicam a origem, destino, trajecto, hora, data, tamanho e duração da comunicação, ou o tipo de serviço subjacente;

p) «Dados informáticos» – Quaisquer dados susceptíveis de processamento por um sistema informático;

q) «Dispositivo» – Qualquer equipamento, material electromagnético, acústico, mecânico, técnico ou outros ou programa de computador;

r) «DSL (Digital Subscriber Line)» - A tecnologia que permite aproveitar o conjunto de pares de cabo de cobre para fins de serviços de *Internet* de banda larga;

s) «Endereço do Protocolo IP» – O conjunto de números que permitem a identificação e a comunicação consistente entre equipamentos (normalmente computadores) de uma rede privada ou pública, mediante uma plataforma de Internet;

t) «Identificador de Célula (Cell ID)» – A identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

u) «IMBI (International Mobile Equipmentidentitv)» – O código pré-gravado nos telefones móveis da tecnologia GSM, que permite a identificação do equipamento ou do terminal a nível internacional, ao ser transmitido ou ao interligar-se a uma rede de comunicações electrónicas

acessíveis ao público. Caso a tecnologia usada não seja GSM considera-se o código equivalente para a tecnologia em questão;

v) «IMSI *(International Mobile Subcriberidentity)*» – O código único de identificação para cada aparelho terminal de telefonia móvel cuja integração no cartão SIM do telemóvel, permite a sua identificação através das redes da tecnologia GSM e UMTS. Caso a tecnologia usada não seja GSM e UMTS considera-se o código equivalente para a tecnologia em questão;

w) «Incidentes informáticos» – Qualquer evento real ou suspeito relacionado com a segurança de sistema informático ou rede;

x) «Intercepção de Comunicação» – O acto destinado a captar dados contidos ou transmitidos através de um sistema de informação mediante o recurso a dispositivos;

y) «Operadores de comunicações electrónicas» – Os organismos, as pessoas colectivas de direito público, as pessoas singulares ou colectivas de direito privado ou misto, que oferecem redes ou serviços de comunicações electrónicas;

z) «Operadores de comunicações electrónicas acessíveis ao público» – São os operadores de redes de comunicações electrónicas públicas e os operadores de serviços de comunicações electrónicas públicos, conforme estes sejam definidos na legislação relevante;

aa) «Prestador de serviço» – Qualquer pessoa, singular ou colectiva, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema de informação, bem como qualquer outra entidade que trate ou armazene dados em nome e por conta daquela ou dos respectivos utilizadores, incluindo, mas não se limitando, a operadores de comunicações electrónicas e prestadores de serviços da sociedade da informação;

bb) «Programa de computador» – O conjunto de instruções (software) usado directa ou indirectamente num computador, tendo em vista a obtenção de determinado resultado, incluindo o material de concepção;

cc) «Rede» – O grupo de sistemas de informação interligados entre si que permite o envio e a recepção de dados;

dd) «Rede do ciberespaço» – Os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos que permitem o envio de sinais por cabo, meios radioeléctricos, meios ópticos, ou por outros meios electromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo *internet)* e móveis os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes utilizadas para a radiofusão sonora e televisiva por cabo, independentemente do tipo de informação transmitida;

ee) «Roubo informático» - Qualquer apropriação indevida de uma rede, sistema informático, bases de dados, equipamento informático, programa informático, usando a violência, ameaça, acesso ilegítimo com vista a estruturação incorrecta de programa ou sistema informático;

ff) «Serviço da sociedade da informação» – O Serviço prestado à distância por via electrónica no âmbito de uma actividade económica na sequência de pedido individual do destinatário, considerando-se, para efeitos da presente definição:

i. «Serviço» – A disponibilização de conteúdos, bens (materiais e imateriais) e serviços, independentemente de a sua entrega ou prestação ser efectuada por via electrónica;

ii. «À distância» – Sem que as partes estejam simultaneamente presentes;

iii. «Por via electrónica» - Enviado da origem e recebido no destino através de meios electrónicos de processamento e de armazenamento de dados, incluindo a via informática, o cabo, rádio, meios ópticos e

meios electromagnéticos, excluindo o telefone, telecópia, telex e teletexto televisivo;

iv. «Pedido individual do destinatário» - A solicitação do destinatário para que lhe seja prestado um serviço da sociedade da informação, incluindo o mero acesso ao sítio ou /página do prestador do serviço da sociedade da informação;

v. Não são serviços da sociedade da informação:

i. Serviços de radiodifusão televisiva e sonora;

ii. Distribuição automática de notas e bilhetes;

iii. Acesso às redes rodoviárias, parques de estacionamento, etc., mediante pagamento, mesmo que existam dispositivos electrónicos à entrada e ou à saída para controlar o acesso ou garantir o correcto pagamento.

gg) «Serviço protegido» – Qualquer serviço da sociedade da informação, com acesso condicional;

hh) «Sistema de informação» – Qualquer dispositivo ou conjunto de dispositivos, bem como a rede que suporta a comunicação entre eles, que, de forma separada ou conjunta, armazenam, tratam, transmitem, recebem ou recuperam dados;

ii) «Sistema informático» – Qualquer dispositivo ou conjunto de dispositivos que procedem o armazenamento, tratamento, recuperação ou transmissão de dados informáticos em execução de um programa de computador;

jj) «Sistema de comunicações electrónicas» – A rede de comunicações electrónicas e qualquer dispositivo ou conjunto de dispositivos que permitem a transmissão de sinais por meio óptico, celular, radioeléctrico, electromagnético ou através de qualquer outra plataforma;

kk) «Sociedade da Informação» – Sociedade em que as principais actividades estão integradas pelas novas tecnologias da informação e comunicação onde a informação circula em redes electrónicas;

ll) «Prestador de serviço» – Qualquer pessoa, singular ou colectiva, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema de informação, bem como qualquer outra entidade que trate ou armazene dados em nome e por conta daquela ou dos respectivos utilizadores. Incluindo, mas não se limitando, a operadores de comunicações electrónicas e prestadores de serviços da sociedade da informação.

ARTIGO 5.º

(Cooperação internacional)

O Estado Angolano deve cooperar com os outros Estados e organizações internacionais em matéria de segurança do ciberespaço nacional para efeitos de prevenção, investigação ou procedimentos respeitantes aos crimes relacionados com os sistemas ou dados informáticos, recolha de prova em suporte electrónico, num restrito respeito, as normas sobre a transferência internacional de dados pessoais, e nos termos e limites do regime jurídico da cooperação internacional em matéria penal, e da protecção de dados pessoais.

ARTIGO 6.º

(Estratégia Nacional de Cibersegurança)

1. A Estratégia Nacional de Cibersegurança estabelece o enquadramento, os objectivos estratégicos e as acções prioritárias do Estado Angolano em matéria de segurança cibernética, em conformidade com as directrizes estratégicas definidas pelas instâncias governamentais competentes.

2. A Estratégia Nacional de Cibersegurança, com vigência de cinco anos, é aprovada pelo Titular do Poder Executivo, após consulta ao Conselho Nacional de Cibersegurança e sob proposta do Centro Nacional de Cibersegurança.
3. A Estratégia Nacional de Cibersegurança é revista de cinco em cinco anos.

CAPÍTULO II
ORGANIZAÇÃO DO SISTEMA NACIONAL DA CIBERSEGURANÇA

SECÇÃO I
DISPOSIÇÕES GERAIS

ARTIGO 7.º
(Estrutura Nacional da Cibersegurança)

A estrutura nacional da Cibersegurança é composta pelas seguintes entidades:

a) O Conselho Nacional de Cibersegurança;
b) O Centro Nacional de Cibersegurança;
c) A Rede Nacional de CSIRTs;
d) Os Operadores de Infra-estruturas Críticas e Serviços Essenciais;
e) Os Prestadores de Serviços Digitais;
f) Os Operadores de Centros de Dados;
g) Os Operadores de Plataformas de Computação em Nuvem;
h) Os Provedores de Serviços de Cibersegurança;
i) Os Operadores de Comunicações Digitais.

SECÇÃO II
CONSELHO NACIONAL DE CIBERSEGURANÇA

ARTIGO 8.º
(Natureza)

O Conselho Nacional de Cibersegurança é um órgão permanente consultivo do Titular do Poder Executivo, de coordenação e articulação entre os diferentes Departamentos Ministeriais ligados, directa e indirectamente, a questões da cibersegurança.

ARTIGO 9.º
(Estrutura, organização e funcionamento)

1. A estrutura, atribuições, organização e funcionamento do Conselho Nacional de Cibersegurança são definidos em diploma próprio.

2. Sem prejuízo do disposto no número anterior, compete ao Conselho Nacional de Cibersegurança:
   a) Assegurar a coordenação político-estratégica para a segurança cibernética;
   b) Supervisionar anualmente a implementação da Estratégia Nacional de Cibersegurança;
   c) Remeter o relatório anual de avaliação da execução da Estratégia Nacional de Cibesegurança à Assembleia Nacional;
   d) Pronunciar-se sobre a aprovação e revisão da Estratégia Nacional de Cibersegurança.

SECÇÃO III
CENTRO NACIONAL DE CIBERSEGURANÇA

ARTIGO 10.º
(Natureza)

O Centro Nacional de Cibersegurança é uma pessoa colectiva de direito público, com autonomia administrativa, financeira e patrimonial, que tem por missão garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes.

ARTIGO 11.º
(Estrutura, organização e funcionamento)

1. A estrutura, atribuições, organização e funcionamento do Centro Nacional de Cibersegurança são definidos em diploma próprio.

2. Sem prejuízo do disposto no número anterior, o Centro Nacional de Cibersegurança exerce as funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias nos termos previstos na presente Lei e no seu Estatuto Orgânico.

SECÇÃO IV
REDE NACIONAL DE CSIRTS

ARTIGO 12.º
(Natureza)

1. A Rede Nacional de CSIRTs é um fórum para partilha de informação de carácter operacional, que assegura a troca de informação sobre incidentes cibernéticos entre o CERT.ao, os CSIRTs sectoriais e institucionais.

2. O ecossistema da Rede Nacional de Resposta a Incidentes informáticos no Ciberespaço tem no topo da sua hierarquia o CERT.ao e pressupõe a criação de CSIRTs sectoriais e institucionais.

3. Os sectores devem adoptar medidas audazes no combate e resiliência aos incidentes e ataques cibernéticos.

4. Os sectores com infra-estruturas críticas e os reguladores dos sectores devem criar os CSIRTs sectoriais e dinamizar o processo de criação de CSIRTs institucionais.

5. Os CSIRTs sectoriais, no âmbito das suas acções de prevenção e combate (resposta) aos abusos no Ciberespaço e ao cibercrime, actuam como elo entre o CERT.ao e CSIRTs institucionais.

6. As equipes de resposta a incidentes cibernéticos institucionais devem velar pela Cibersegurança nas respectivas instituições, prestando serviços de assistência ao utilizador final, o cidadão e as instituições, e devem colaborar com os CSIRTs dos respectivos sectores.

SECÇÃO V
OPERADORES DE INFRA-ESTRUTURAS CRÍTICAS E SERVIÇOS ESSENCIAIS

SUBSECÇÃO I
OPERADORES DE INFRA-ESTRUTURAS CRÍTICAS

ARTIGO 13.º
(Natureza)

Operador de Infra-estrutura Crítica é uma entidade pública ou privada que opera uma infra-estrutura crítica.

ARTIGO 14.º
(Obrigações dos Operadores de Infra-estruturas Críticas)

1. São obrigações dos 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) Informar ao CERT.ao sobre ciberameaças e ciberataques que registem na sua actividade;
h) 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 no Centro Nacional de Cibersegurança.

SUBSECÇÃO II
OPERADORES DE SERVIÇOS ESSENCIAIS

ARTIGO 15.º
(Natureza)

Os operadores de serviços essenciais enquadram-se num dos tipos de entidades que actuam nos sectores e subsectores e como tal definidos em diploma próprio.

ARTIGO 16.º
(Obrigações dos Operadores de Serviços Essenciais)

O operador do serviço essencial implementa um sistema de gestão da segurança no sistema de informação utilizado para prestar um serviço essencial, garantindo:

a) Realizar a avaliação sistemática do risco de ocorrência de incidentes e gerenciar esse risco;
b) Implementar medidas técnicas e organizacionais apropriadas e proporcionais, levando em consideração o estado mais recente dos conhecimentos, incluindo:

i. Manutenção e operação segura do sistema de informação;
ii. Segurança física e ambiental, incluindo o controlo do acesso;
iii. Segurança e continuidade das prestações de serviços de que depende a prestação do serviço essencial;
iv. Implementar, documentar e manter planos de acção que permitam a prestação contínua e ininterrupta do serviço essencial e que garantam a confidencialidade, integridade, disponibilidade e autenticidade das informações;
v. Cobrir o sistema de informação utilizado para a prestação do serviço essencial com um sistema de monitorização contínua.

c) Colectar informações sobre ameaças à cibersegurança e vulnerabilidades a incidentes do sistema de informação utilizado para prestar o serviço-chave;
d) Gerenciar incidentes;
e) Aplicar medidas para prevenir e limitar o impacto de incidentes na segurança do sistema de informação utilizado para prestar o serviço essencial, incluindo:
i. Utilização de mecanismos que garantam a confidencialidade, integridade, disponibilidade e autenticidade dos dados tratados no sistema de informação;
ii. Cuidado das actualizações de software;
iii. Protecção contra modificações não autorizadas no sistema de informação;
iv. Tomada das medidas imediatas quando forem identificadas vulnerabilidades ou ameaças à cibersegurança.
f) Utilizar meios de comunicação que permitam uma comunicação adequada e segura no âmbito do sistema nacional de cibersegurança.

SECÇÃO VI
PRESTADORES DE SERVIÇOS DIGITAIS

ARTIGO 17.º
(Natureza)

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

ARTIGO 18.º
(Obrigações dos Prestadores de Serviços Digitais)

1. São obrigações dos 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) Informar ao CERT.ao sobre ciberameaças e ciberataques que registem na sua actividade;
   e) Manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados.

2. Para o exercício das suas actividades no território nacional os Operadores de Plataformas Digitais devem registar-se no Centro Nacional de Cibersegurança.

3. Os Operadores de Plataformas Digitais que prestam serviços ao Estado estão sujeitos a regulamentação específica.

SECÇÃO VII
OPERADORES DE CENTROS DE DADOS

ARTIGO 19.º
(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 20.º
(Obrigações dos Operadores de Centro de Dados)

1. São obrigações dos Operadores de Centro 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) Informar ao CERT.ao sobre ciberameaças e ciberataques que registem na sua actividade;
   f) 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 no território nacional, os Operadores de Centros de Dados devem registar-se no Centro Nacional de Cibersegurança.

3. Os Operadores de Centros de Dados que prestam serviços ao Estado estão sujeitos a regulamentação específica.

SECÇÃO VIII
OPERADORES DE PLATAFORMAS DE COMPUTAÇÃO EM NUVEM

ARTIGO 21.º
(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 22.º
(Obrigações de Operadores de Plataformas de Computação em Nuvem)

1. São obrigações dos Operadores de Plataformas de Computação em Nuvem:
   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) Informar ao CERT.ao sobre ciberameaças e ciberataques que registem na sua actividade;
f) 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 no território nacional, os Operadores de Plataformas de Computação em Nuvem devem registar-se no Centro Nacional de Cibersegurança.

3. Os Operadores de Serviço de Computação em Nuvem Privada que prestam serviços ao Estado estão sujeitos a regulamentação específica.

SECÇÃO IX
PROVEDORES DE SERVIÇOS DE CIBERSEGURANÇA

ARTIGO 23.º
(Natureza)

O Provedor de Serviço de Cibersegurança 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 cibersegurança.

ARTIGO 24.º

(Obrigações dos Prestadores de Serviços de Cibersegurança)

1. São obrigações dos Prestadores de Serviços de Cibersegurança:
   a) Comunicar de imediato ao Centro Nacional de Cibersegurança e ao CERT.ao 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) Informar ao CERT.ao sobre ciberameaças e ciberataques que registem na sua actividade;
   f) 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 no território nacional os Prestadores de Cibersegurança devem registar-se no Centro Nacional de Cibersegurança.

SECÇÃO XI
OPERADORES DE COMUNICAÇÕES DIGITAIS

ARTIGO 25.º

(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 26.º

(Obrigações dos Operadores de Comunicações Digitais)

1. São obrigações dos 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) Informar ao CERT.ao sobre ciberameaças e ciberataques que registem na sua actividade;
   g) Manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados.

2. Para o exercício das suas actividades no território nacional os Operadores de Comunicações Digitais devem registar-se no Centro Nacional de Cibersegurança.

CAPÍTULO III
SEGURANÇA DAS REDES E DOS SISTEMAS DE INFORMAÇÃO

SECÇÃO I
DISPOSIÇÕES GERAIS

ARTIGO 27.º
(Segurança de Redes de Comunicação de Dados)

As redes do espaço cibernético devem assegurar a integridade, a confidencialidade e a privacidade das comunicações, mediante a implementação de serviços de segurança lógica.

ARTIGO 28.º
(Segurança da Internet)

1. A comunicação de dados na rede Internet deve assegurar a integridade, a confidencialidade e a privacidade dos sistemas de informação, mediante a implementação de serviços de segurança lógica e física, estabelecidas nos padrões e normas definidas pelos organismos internacionais que regem a organização e o funcionamento da Internet.

2. Sem prejuízo dos termos e condições aplicáveis para utilização específica do espaço cibernético, os operadores e prestadores de serviços de Internet devem promover o registo dos utilizadores e a execução de medidas e instrumentos necessários à antecipação, à detecção, a reacção e a recuperação em situações de riscos de segurança, nas redes.

ARTIGO 29.º

(Protecção do Sistema de Nomes de Domínio)

1. É necessário 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. O disposto no número anterior é objecto de regulamentação específica, estabelecida no regime jurídico das comunicações electrónicas.

ARTIGO 30.º

(Cooperação institucional)

O Centro Nacional de Cibersegurança deve estabelecer relações de cooperação institucional com organismos públicos e privados e outras congéneres internacionais na promoção da protecção e segurança do ciberespaço nacional.

SECÇÃO II
REQUISITOS DE SEGURANÇA E NOTIFICAÇÃO DE INCIDENTES

ARTIGO 31.º

(Incidentes de segurança cibernética de impacto significativo)

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

a) Impacto do incidente de cibersegurança, classificado em menos ou mais grave, de acordo com o grau de consequências determinado na avaliação do risco realizado;
b) Devido ao incidente de cibersegurança, 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 serviço;
c) A continuidade do serviço de algum outro prestador de serviço essencial é interrompida devido ao incidente de cibersegurança;
d) Para resolver o incidente de cibersegurança, 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 cibersegurança.

2. O disposto no número anterior é objecto de regulamentação própria.

ARTIGO 32.º

(Requisitos de segurança e normalização)

1. Os requisitos de segurança são definidos de forma a permitir a utilização de padrões, normas e especificações técnicas internacionalmente aceites, aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.

2. Os requisitos de segurança são definidos nos termos do diploma próprio.

ARTIGO 33.º
(REQUISITOS DE NOTIFICAÇÃO DE INCIDENTES)

1. As entidades sujeitas aos requisitos de notificação de incidentes são as seguintes:
   a) Administração Pública;
   b) CSIRTs sectoriais e CSIRTs institucionais;
   c) Operadores de Infra-estruturas Críticas;
   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 utilizem redes e sistemas de informação.

2. Sem prejuízo do disposto na presente lei, os requisitos de notificação de incidentes são definidos nos termos previstos em diploma próprio.

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 entidades que superintendem as áreas da Defesa e Segurança Nacional e da Ordem e Segurança pública;
   b) Às redes e sistemas de informação que processem informação classificada conforme a legislação específica.

ARTIGO 34.º

(Requisitos de segurança para a Administração Pública e Operadores de Infra-estruturas Críticas)

1. Os Órgãos e Serviços da Administração Pública e os Operadores de Infra-estruturas Críticas devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.

2. As medidas 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 Órgãos e Serviços da Administração Pública e os Operadores de Infra-estruturas Críticas tomam as medidas adequadas para evitar os incidentes que afectem a segurança das redes e dos sistemas de informação utilizados e para reduzir ao mínimo o seu impacto.

ARTIGO 35.º

(Notificação de incidentes para a Administração Pública e Operadores de Infra-estruturas Críticas)

1. Os Órgãos e Serviços da Administração Pública e os Operadores de Infra-estruturas Críticas devem estabelecer CSIRTs institucionais e notificar ao respectivo CSIRT sectorial e ao CERT.ao os incidentes com um impacto relevante na segurança das redes e dos sistemas de informação, no prazo definido em diploma próprio aprovado pelo Centro Nacional de Cibersegurança.

2. A notificação dos Operadores de Infra-estruturas Críticas inclui informação que permita ao CERT.ao determinar o impacto transfronteiriço 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 são tidos em conta, designadamente, 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. Sempre que as circunstâncias o permitam, o Centro Nacional de Cibersegurança presta ao notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente, informações que possam contribuir para o tratamento eficaz do incidente.

6. O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público, salvaguardando a segurança e os interesses dos Operadores de Infra-estruturas Críticas.

7. Os Órgãos e Serviços da Administração Pública e os Operadores de Infra-estruturas Críticas são obrigados a submeter ao CSIRT sectorial e para o CERT.ao o relatório mensal sobre a resposta e resolução do incidente.

8. O relatório de resposta e resolução de incidentes incluirá informações sobre as causas do incidente de segurança cibernética, o tempo gasto na sua resolução, as medidas aplicadas, o impacto da mesma e todas as outras informações exigidas pelos regulamentos da presente lei.

ARTIGO 36.º

(Requisitos de segurança para os Operadores de Serviços Essenciais)

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

2. As medidas 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 afectem a segurança das redes e dos sistemas de informação utilizados para a prestação dos seus serviços essenciais e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços.

ARTIGO 37.º

(Notificação de incidentes para os Operadores de Serviços Essenciais)

1. Os Operadores de Serviços Essenciais devem estabelecer CSIRTs institucionais e notificar ao respectivo CSIRT sectorial e ao CERT Nacional os incidentes com um impacto relevante na continuidade dos

serviços essenciais por si prestados, no prazo definido pelo Centro Nacional de Cibersegurança.

2. A notificação inclui informação que permita ao Centro Nacional de Cibersegurança determinar o impacto transfronteiriço 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 são tidos em conta, designadamente, os seguintes parâmetros:
   a) O número de utilizadores afectados pela perturbação do serviço essencial;
   b) A duração do incidente;
   c) A distribuição geográfica, no que se refere à zona afectada pelo incidente.

5. Com base na informação prestada na notificação, o Centro Nacional de Cibersegurança informa os pontos de contacto únicos dos outros Estados afectados, caso o incidente tenha um impacto importante na continuidade dos serviços essenciais nesses Estados Membros.

6. No caso referido no número anterior, o Centro Nacional de Cibersegurança salvaguarda a segurança e os interesses do Operador de Serviços Essenciais, bem como a confidencialidade da informação prestada na sua notificação.

7. Sempre que as circunstâncias o permitam, o Centro Nacional de Cibersegurança presta ao Operador de Serviços Essenciais notificante as

informações relevantes relativas ao seguimento da sua notificação, nomeadamente, informações que possam contribuir para o tratamento eficaz do incidente.

8. O Centro Nacional de Cibersegurança transmite as notificações referidas no n.º 1 do presente artigo, aos pontos de contacto únicos dos outros Estados afectados.

9. O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar informação relativa a incidentes específicos de acordo com o interesse público.

10. Se um Operador de Serviços Essenciais depender de um terceiro prestador de serviços digitais para a prestação de um serviço essencial, notifica todos os impactos importantes na continuidade dos seus serviços, decorrentes dos incidentes que afectem o prestador de serviços digitais.

11. Os Operadores de Serviços Essenciais são obrigados a submeter ao CSIRT sectorial e para o CERT.ao o relatório mensal sobre a resposta e resolução do incidente.

12. O relatório de resposta e resolução de incidentes incluirá informações sobre as causas do incidente de cibersegurança, o tempo gasto na sua resolução, as medidas aplicadas, o impacto da mesma e todas as outras informações exigidas pelos regulamentos da presente lei.

ARTIGO 38.º

(Requisitos de Segurança para os Prestadores de Serviços Digitais)

1. Os Prestadores de Serviços Digitais identificam e devem tomar as medidas técnicas, organizativas, 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 referidas no número anterior 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 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 Prestadores de Serviços Digitais devem tomar medidas para evitar os incidentes que afectem 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.

4. Os elementos constantes dos números anteriores são objecto de diploma próprio.

ARTIGO 39.º

(Notificação de incidentes para os Prestadores de Serviços Digitais)

1. Os Prestadores de Serviços Digitais devem notificar ao respectivo CSIRT sectorial e ao CERT.ao os incidentes com um impacto relevante

na continuidade dos serviços essenciais por si prestados, no prazo definido pelo Centro Nacional de Cibersegurança.

2. A notificação referida no número anterior inclui informação que permita ao Centro Nacional de Cibersegurança 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 obrigação de notificar um incidente só se aplica se o prestador de serviços digitais tiver acesso à informação necessária para avaliar o impacto de um incidente em função dos factores dos requisitos de segurança para estes prestadores a que se refere a presente Lei.

6. Caso os incidentes referidos no n.º 1 digam respeito a dois ou mais Estados, o Centro Nacional de Cibersegurança informa os pontos de contacto únicos dos outros Estados afectados.

7. No caso referido no número anterior, o Centro Nacional de Cibersegurança salvaguarda a segurança e os interesses do prestador de serviços digitais.

8. O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público.

9. Os Prestadores de Serviços Digitais são obrigados a submeter ao CSIRT sectorial e para o CERT.ao o relatório mensal sobre a resposta e resolução do incidente.

10. 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, o impacto da mesma e todas as outras informações exigidas pelos regulamentos desta Lei.

ARTIGO 40.º

(Requisitos de segurança para Operadores de Centros de Dados)

1. Os Operadores de Centros de Dados devem tomar medidas adequadas para garantir a integridade, confidencialidade e a disponibilidade dos dados armazenados, reduzindo os riscos de tempo de inactividade.

2. Os Operadores de Centros de Dados devem ser licenciados pelo Centro Nacional de Cibersegurança.

ARTIGO 41.º

(Notificação de incidentes para Operadores de Centros de Dados)

1. Os Operadores de Centros de Dados devem 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.

2. Os Operadores de Centros de Dados devem notificar ao CERT.ao atempadamente de qualquer incidente de cibersegurança ou vazamento de dados, incluindo dados pessoais, de que tenha conhecimento e o que afecta ou pode afectar o conteúdo do assinante.

3. Os Operadores de Centros de Dados devem notificar aos assinantes de qualquer cobertura de seguro fornecido pelo serviço contra qualquer responsabilidade civil para esses assinantes.

4. As informações relacionadas à cobertura de seguro devem incluir as características básicas necessárias para os assinantes dos serviços avaliarem a sua exposição ao risco e tomar uma decisão sobre a sua cobertura e conformidade do seguro.

5. Os Operadores de Centros de Dados devem 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.

6. Os Operadores de Centros de Dados são obrigados a submeter ao CSIRT sectorial e para o CERT.ao o relatório mensal sobre a resposta e resolução do incidente.

7. O relatório de resposta e resolução de incidentes inclui informações sobre as causas do incidente de cibersegurança, o tempo gasto na sua resolução, as medidas aplicadas o impacto da mesma e todas as outras informações exigidas pelos regulamentos desta Lei.

ARTIGO 42.º

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

1. As entidades devem avaliar aspectos de segurança quanto ao armazenamento de dados na nuvem para garantir o acesso conforme o recomendado pela indústria, para manter as configurações de gestão de conformidade e para assegurar que as boas práticas estão sendo adoptadas e cumpridas.

2. Os requisitos de segurança são definidos em diploma próprio.

ARTIGO 43.º

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

1. Os Provedores de Serviços de Computação em Nuvem devem notificar aos seus assinantes, sem atraso injustificado de quaisquer incidentes de cibersegurança, incluindo vazamento de dados e o que afecta ou pode afectar o conteúdo do assinante, dados ou quaisquer serviços fornecidos a esses assinantes.

2. Os Provedores de Serviços de Computação em Nuvem devem notificar ao CERT.ao de imediato de qualquer incidente de cibersegurança e

vazamento de dados, incluindo dados pessoais, de que tenha conhecimento.

3. Os Provedores de Serviços de Computação em Nuvem devem notificar aos assinantes de qualquer cobertura de seguro fornecida pelo serviço contra qualquer responsabilidade civil para esses assinantes.

4. As informações relacionadas à cobertura de seguro devem incluir, pelo menos, as características básicas que possam ser, razoavelmente, necessárias para os assinantes avaliar sua exposição ao risco e tomar uma decisão sobre a cobertura de seguro e conformidade.

5. Os Provedores de Serviços de Computação em Nuvem devem adoptar regras e políticas internas para a continuidade do negócio, recuperação de desastres e gestão de riscos e fornecer aos assinantes dos serviços um resumo dessas regras e políticas.

6. Os Operadores de Plataformas de Computação em Nuvem são obrigados a submeter ao CSIRT Sectorial e ao CERT.ao, o relatório mensal sobre a resposta e resolução do incidente.

7. O relatório de resposta e resolução de incidentes inclui informações sobre as causas do incidente de cibersegurança, o tempo gasto na sua resolução, as medidas aplicadas, o impacto da mesma e todas as outras informações exigidas pelos regulamentos desta Lei.

ARTIGO 44.º

(Notificação voluntária de incidentes)

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

2. 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.

CAPÍTULO IV
(RESPOSTAS À AMEAÇAS E INCIDENTES DE CIBERSEGURANÇA)

ARTIGO 45.º

(Acções para prevenir e gerir incidentes de cibersegurança)

Sempre que o CERT.ao receber informações sobre uma ameaça ou incidente de cibersegurança de alto impacto significativo, deve informar a entidade ou órgão regulador sectorial competente ou ao CSIRT Sectorial correspondente, para que, no exercício das competências estabelecidas nesta lei, realizar todas as acções que forem necessárias para prevenir e gerir a ameaça ou incidente de cibersegurança em uma infra-estrutura crítica, buscando:

a) Avaliar o impacto ou potencial impacto da ameaça ou incidente;
b) Eliminar a ameaça de cibersegurança ou prevenir qualquer dano ou dano adicional resultante do incidente de cibersegurança;
c) Impedir que um novo incidente de cibersegurança surja dessa ameaça ou do incidente de cibersegurança.

ARTIGO 46.º

(Responsabilidade pela notificação de incidente de cibersegurança)

Caso as informações sobre um incidente de cibersegurança de impacto significativo sejam inicialmente recebidas por um CSIRT Sectorial, este será responsável por notificar ao CERT.ao, para que possa ser correlacionado com outros incidentes significativos reportados de outros Sectores de Infra-estrutura Crítica.

ARTIGO 47.º

(Meios de prevenção e gestão de incidentes)

As acções mencionadas na presente lei permitem que o CERT. ao ou CSIRT Sectorial, se houver, tome as seguintes medidas para proteger a cibersegurança da Infra-estrutura Crítica:

a) Exigir ao Operador de Infra-estrutura Crítica que informe sobre qualquer incidente de cibersegurança de alto impacto significativo pelo qual é afectado;
b) Exigir ao Operador de Infra-estrutura Crítica ou ao Operador de Sistema de Informação vinculado ao referido Operador, que realize medidas correctivas e/ou preventivas, para responder ao incidente de acordo com o regulamento correspondente;
c) Solicitar ao Operador de um Sistema de Informação ligado ao Operador de uma Infra-estrutura Crítica que realize qualquer acção dentro da estrutura para ajudar na gestão de incidentes de cibersegurança:
    i. Reservar o estado do sistema de informação;
    ii. Monitorar o sistema de informação por um período de tempo específico;
    iii. Realizar uma análise do sistema de informação para detectar vulnerabilidades de cibersegurança, avaliar a maneira e a extensão

do sistema de informação afectado pelo incidente de cibersegurança.

ARTIGO 48.º

(Entrega de informações)

1. A entrega das informações exigidas pelo CSIRT Institucional e caso não haja, pelo CSIRT Sectorial e caso não haja, pelo CERT.ao, em virtude dos seus poderes para gerir e prevenir incidentes de cibersegurança, não serão considerados como uma quebra de confidencialidade previamente estabelecida por leis, regulamentos, contractos ou códigos de conduta profissional.

2. As informações que são entregues ao CSIRT Sectorial ou CERT.ao são considerados reservadas e confidenciais.

3. Caso o sistema de informação esteja comprometido por uma ameaça ou incidente de cibersegurança iminente, que pode prejudicá-lo ou destruí-lo significativamente, o CSIRT Sectorial, caso não haja, o CERT.ao deve suspender imediatamente o uso deste sistema ou qualquer um dos seus componentes até que a causa da ameaça seja eliminada.

ARTIGO 49.º

(Divulgação Responsável de Vulnerabilidades)

1. Qualquer 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, contractos 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, quando:
   a) 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) No processo de identificação, a pessoa tomou as precauções necessárias para prevenir incidentes referentes à privacidade, degradação ou falhas no serviço, destruição ou manipulação dos dados;
   d) 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:
   a) Negação de serviço;
   b) Evidência física;
   c) Uso de código malicioso e engenharia social;
   d) Alteração, remoção ou destruição de dados.

CAPÍTULO V
(FUNDO NACIONAL DE CIBERSEGURANÇA)

ARTIGO 50.º
(Natureza)

1. É instituído pela presente lei um Fundo Nacional de Cibersegurança com o objectivo de fornecer recursos financeiros para promover e fortalecer a cibersegurança do País.

2. O Fundo Nacional de Cibersegurança é gerido pelo Centro Nacional de Cibersegurança.

3. As entidades registadas e licenciadas para a prestação de serviços de TIC devem contribuir para o Fundo Nacional de Cibersegurança.

4. As regras de funcionamento do Fundo Nacional de Cibersegurança são estabelecidas em diploma próprio.

ARTIGO 51.º
(Objectivos)

São objectivos do Fundo Nacional de Cibersegurança:

a) Incrementar os recursos financeiros destinados à promoção da cibersegurança, 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 Executivo em matérias de cibersegurança;
c) Promover a formação contínua para o desenvolvimento de capacidade nacional em matérias de cibersegurança.

ARTIGO 52.º

(Beneficiários)

São beneficiários do Fundo Nacional de Cibersegurança:

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 públicas ou privadas que contribuem ao Fundo Nacional de Cibersegurança, através do acesso a programas de formação contínua, para actualização tecnológica em matérias de cibersegurança;
c) As Entidades do Sistema Nacional de Cibersegurança 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 públicas ou privadas que pretendam institucionalizar CSIRTs sectoriais e institucionais.

ARTIGO 53.º

(Fontes de receitas)

1. Constituem fontes de receitas do Fundo Nacional de Cibersegurança:
    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 cibersegurança;
    c) As entidades públicas e privadas que integram o Sistema Nacional de Cibersegurança, licenciadas para o exercício da actividade de prestação de serviços de cibersegurança, que 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 54.º

(Gestão)

O Centro Nacional de Cibersegurança é responsável pela gestão do Fundo, de acordo com a Lei do Orçamento Geral do Estado.

CAPÍTULO VI
(SUPERVISÃO, FISCALIZAÇÃO, AUDITORIA E REGIME DE RESPONSABILIDADE)

SECÇÃO I
(SUPERVISÃO, FISCALIZAÇÃO E AUDITORIA)

ARTIGO 55.º

(Supervisão)

Compete ao Centro Nacional de Cibersegurança garantir a supervisão dos sectores abrangidos pela presente lei.

ARTIGO 56.º

(Fiscalização)

Compete ao Centro Nacional de Cibersegurança realizar acções de fiscalização das redes e sistemas informáticos, com vista a garantir cibersegurança.

ARTIGO 57.º

(Auditoria)

O Centro Nacional de Cibersegurança estabelece os padrões técnicos que servem de base para realização de auditoria de cibersegurança e de segurança de informação, nos termos a regulamentar.

SECÇÃO II
(CONTRA-ORDENAÇÕES E SANÇÕES)

ARTIGO 58.º

(Contra-ordenações)

1. As infracções ao disposto na presente lei constituem contra-ordenações, nos termos dos artigos seguintes.

2. Sem prejuízo do disposto no número anterior, se o mesmo facto constituir, simultaneamente, crime e contra-ordenação, o agente é punido sempre a título de crime, nos termos previstos na legislação penal, sem prejuízo da aplicação da coima correspondente nos termos da presente Lei.

Artigo 59.º

(Espécies de contra-ordenações)

As entidades abrangidas pelo presente diploma, que violarem as disposições estabelecidas nos artigos anteriores, estão sujeitas às contra-ordenações resultantes dos seguintes factos:

a) Incumprimento da obrigação de implementar os requisitos de segurança tal como previstos na presente Lei;

b) Falta de notificação de incidentes ao CERT.ao no prazo estipulado em diploma próprio aprovado pelo Centro Nacional de Cibersegurança;
c) Omissão ou falsificação de informações nos relatórios de auditoria ou gestão de riscos, tal como previstos na presente lei;
d) Falta de elaboração ou manutenção do Plano de Resposta a Incidentes, nos casos como tal exigidos;
e) Não submissão de relatórios periódicos dentro do prazo estabelecido na presente Lei;
f) Violação das disposições relativas à confidencialidade e protecção da informação;
g) Não cumprimento das obrigações contratuais de segurança por parte dos fornecedores de tecnologia e serviços.

ARTIGO 60.º

(Advertência e coimas)

1. As contra-ordenações previstas na presente Lei são punidas da seguinte forma:
   a) Advertência, em caso de contra-ordenações leves ou primeira contra-ordenação com impacto reduzido;
   b) Coima, dependendo da gravidade da contra-ordenação e do impacto na segurança das redes e sistemas de informação;

2. O valor da coima é fixado da seguinte forma:
   a) Para pessoas singulares, o montante mínimo é de 100 salários mínimas nacionais e o máximo de 3 000 salários;
   b) Para pessoas colectivas, o montante mínimo é de 500 salários mínimas nacionais e o máximo de 30 000.

3. As coimas aplicáveis por contra-odernações à presente lei devem ser pagas em moeda nacional, no prazo máximo de 30 (trinta) dias, contados a partir da data de notificação da decisão que as aplicou.

ARTIGO 61.º

(Sanções Acessórias)

As contra-ordenações podem ser simultaneamente punidas com coima e com as seguintes sanções acessórias:

a) Suspensão temporária de actividades até que a entidade cumpra os requisitos estabelecidos, em caso de reincidência ou contra-ordenações graves;
b) Proibição de contratação pública por um período de até 5 anos, em casos de contra-ordenação grave ou contínua que comprometa infra-estruturas críticas ou a segurança nacional.

ARTIGO 62.º

(Agravação e atenuação das coimas e sanções acessórias)

1. As coimas e sanções acessórias podem ser atenuadas se a entidade abrangida pelo diploma demonstrar proactividade na correcção das contra-ordenações ou colaboração activa com o CERT.ao na mitigação de riscos.

2. As coimas e sanções acessórias são agravadas ao dobro se a contra-ordenação envolver negligência grave, dolo ou resultar em danos significativos a terceiros, infra-estruturas críticas ou à segurança nacional.

ARTIGO 63.º

(Competência para fiscalização e aplicação de sanções)

Sem prejuízo do disposto na legislação sobre a protecção de dados pessoais, as competências de fiscalização e de aplicação das sanções previstas na presente lei cabem ao Centro Nacional de Cibersegurança.

ARTIGO 64.º

(Procedimento Sancionatório)

1. A aplicação das sanções será precedida de um processo contra-ordenacional, durante o qual a entidade infractora terá direito ao contraditório e à ampla defesa.

2. O processo sancionatório será instaurado pelo Centro Nacional de Cibersegurança, que notificará a entidade para apresentar defesa no prazo de 15 dias úteis.

3. As decisões sancionatórias serão comunicadas por escrito, devendo incluir a descrição dos factos, a infracção cometida, as sanções aplicadas e os prazos para recurso.

4. Cabe recurso das decisões emitidas pelo Centro Nacional de Cibersegurança, nos termos gerais previstos no Código do Procedimento Administrativo e na demais legislação competente sobre a matéria.

ARTIGO 65.º

(Produto das coimas)

Os valores arrecadados obedecem a seguinte repartição:

a) 40%, a favor do Tesouro Nacional;
b) 60%, a favor do CERT.ao.

SECÇÃO III

RESPONSABILIDADE CRIMINAL E CIVIL

ARTIGO 66.º

(Responsabilidades penal e concurso com contra-ordenação)

1. O acesso ilegítimo a dados ou divulgação indevida de informações confidenciais constituem crimes contra a cibersegurança e são puníveis nos termos da legislação penal, sem prejuízo das coimas e sanções acessórias cabíveis nos termos da presente Lei.

2. Em caso de concurso de entre um crime e uma contra-ordenação, o tribunal que julgar o crime pode também aplicar a coima e as medidas acessórias estabelecidas na presente lei, salvo se o Centro Nacional de Cibersegurança as tiver já aplicado ou existir um processo de contra-ordenação pendente.

ARTIGO 67.º

(Responsabilidade Civil Objectiva)

1. Constitui-se na obrigação de reparar os danos ou de indeminizar os lesados, aquele que em função de uma conduta violadora da presente lei, independentemente de culpa, tenha causado danos a terceiros ou infra-estruturas críticas ou à segurança nacional.

2. Havendo uma relação entre o comitente e comissão a responsabilidade civil é solidária, nos termos da lei geral.

ARTIGO 68.º

(Responsabilidade Civil Conexa com a Penal)

1. A responsabilidade civil é independente da responsabilidade penal.

2. Constituindo-se o facto gerador de responsabilidade cível um crime, o pedido cível de indemnização pode ser deduzido no âmbito do processo crime e corre por apenso a este nos termos da lei processual penal.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

ARTIGO 69.º

(Regime subsidiário)

1. Em matéria contra-ordenacional, em tudo o que não estiver previsto na presente Lei, aplica -se o disposto no regime geral das contra-ordenações.

2. Aos crimes contra os sistemas informáticos, aplica-se subsidiariamente o regime jurídico previsto na Legislação Penal e Processual Penal.

ARTIGO 70.º

(Dúvidas e omissões)

As dúvidas e omissões que resultarem da interpretação e da aplicação da presente Lei são resolvidas pela Assembleia Nacional.

ARTIGO 71.º

(Revogação)

É revogada toda a legislação que contrarie o disposto na presente lei, nomeadamente a Lei n.º 7/17, de 16 de Fevereiro.

ARTIGO 72.º

(Entrada em vigor)

A presente Lei entra vem vigor à data da sua publicação.

Vista e aprovada pela Assembleia Nacional, em Luanda, aos _____ de _____ de 2024.

A Presidente da Assembleia Nacional, *Carolina Cerqueira.*

Promulgada aos ____ de _____ de 2024.

Publique-se.

O Presidente da República, JOÃO MANUEL GONÇALVES LOURENÇO.