

Lei n.º 9/26, de 28 de Setembro

Lei da Cibersegurança · República de Angola

Diário da República, I série, n.º 183, de 28 de Setembro de 2026, páginas 7266 a 7290. Aprovada pela Assembleia Nacional a 12 de Agosto de 2026, promulgada a 8 de Setembro de 2026, em vigor desde 28 de Setembro de 2026. Revoga a Lei n.º 7/17, de 16 de Fevereiro.

Transcrição verificada página a página pelo portal Lei Ciber AO (leiciber.ao). Serve para pesquisa e citação; em caso de divergência prevalece o Diário da República. Conteúdo informativo, não constitui aconselhamento jurídico.

Índice

Capítulo I, Disposições gerais (artigos 1.º a 8.º)

Capítulo II, Sistema Nacional da Cibersegurança (artigos 9.º a 24.º)

Capítulo III, Segurança das redes e dos sistemas de informação (artigos 25.º a 43.º)

Capítulo IV, Resposta a ameaças e incidentes de cibersegurança (artigos 44.º a 49.º)

Capítulo V, Supervisão, fiscalização e auditoria (artigos 50.º a 52.º)

Capítulo VI, Responsabilidade (artigos 53.º a 62.º)

Capítulo VII, Disposições finais e transitórias (artigos 63.º a 67.º)

Considerando que, de acordo com a Constituição, a segurança nacional visa a garantia da salvaguarda do Estado e o asseguramento da estabilidade e do desenvolvimento contra quaisquer ameaças e riscos;

Tendo em conta à necessidade de reforçar a resiliência do ciberespaço nacional, de suportar a crescente transformação digital da sociedade, da economia e da Administração Pública e de assegurar a protecção das redes e dos sistemas de informação, das infra-estruturas críticas e dos serviços essenciais, através da prevenção, detecção, resposta e recuperação de incidentes cibernéticos, sem prejuízo do respeito pelos direitos, liberdades e garantias fundamentais;

Havendo a necessidade de estabelecer o quadro legal regulador da cibersegurança no território angolano;

A Assembleia Nacional aprova, por mandato do povo, nos termos da alínea b) do artigo 161.º e do n.º 2 do artigo 165.º, conjugados com a alínea d) do n.º 2 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, visando proteger os cidadãos e as instituições, públicas e privadas contra ciberameaças e ciberataques, bem como assegurar a integridade, a disponibilidade, a autenticidade e a confidencialidade das redes, dos sistemas de informação, das infra-estruturas críticas e dos serviços essenciais do País, com respeito pelos princípios fundamentais e pelos direitos, liberdades e garantias constitucionalmente consagrados.

Artigo 2.º

(Âmbito)

1. A presente Lei aplica-se a todas pessoas singulares e colectivas, públicas e privadas, que utilizem o ciberespaço angolano.
2. A presente Lei aplica-se, ainda, aos actos praticados no território nacional e fora dele, desde que se destinem ao ciberespaço angolano.

Artigo 3.º

(Ciberdefesa e ordem interna)

1. As matérias relativas à ciberdefesa e ordem interna são reguladas em diploma próprio.
2. As entidades que tratam das matérias referidas no número anterior cooperam institucionalmente com as entidades civis competentes pela cibersegurança.

Artigo 4.º

(Tratamento de dados pessoais)

1. Os órgãos que integram o Sistema Nacional de Cibersegurança, nos termos do artigo 10.º, podem proceder ao tratamento de dados pessoais na medida do estritamente necessário para assegurar o cumprimento das obrigações legais e a prossecução de missões de interesse público ou de autoridade pública em que estão investidos, nos termos da

presente Lei e da Lei da Protecção de Dados Pessoais.

2. O tratamento de dados pessoais a que se refere o número anterior visa:

- a) Evitar a consumação de uma ciberameaça significativa para a segurança das redes e sistemas de informação;
- b) Responder eficazmente a um incidente de cibersegurança.

Artigo 5.º

(Protecção da correspondência e das comunicações)

1. É inviolável o sigilo da correspondência e dos demais meios de comunicação privada, nos termos da Constituição.

2. Apenas por decisão judicial competente proferida nos termos da lei, é permitida a ingerência das autoridades públicas na correspondência e nos demais meios de comunicação privada.

Artigo 6.º

(Dever geral de informação e diligência)

1. Os cidadãos e instituições envolvidos em ameaças ou incidentes de cibersegurança susceptíveis de comprometer a segurança das redes e sistemas de informação devem comunicá-las imediatamente às autoridades competentes ou às entidades responsáveis pelos sistemas afectados ou em risco.

2. Todos devem adoptar comportamentos responsáveis na utilização do ciberespaço, respeitando as normas de cibersegurança estabelecidas na presente Lei e demais legislação aplicável.

Artigo 7.º

(Definições)

Por efeitos do presente Lei, considera-se:

- a) «Assinante»: pessoa singular ou colectiva que é parte num contrato com um operador de comunicações electrónicas acessíveis ao público;
- b) «CERT.ao (Equipa Nacional de Resposta a Emergências Informáticas)»: Estrutura operacional do Centro Nacional de Cibersegurança;
- c) «Ciberameaça»: acção, circunstância, evento ou conduta intencional ou accidental, susceptível de comprometer a confidencialidade, integridade, autenticidade e disponibilidade de sistemas de informação, redes, infra-estruturas críticas e dados no ciberespaço;
- d) «Ciberameaça Significativa»: uma ciberameaça que, com base nas suas características técnicas, possa ser considerada susceptível de ter um impacto grave nas redes e sistemas de informação de uma entidade ou dos utilizadores dos serviços com risco de causar danos materiais ou imateriais consideráveis;
- e) «Ciberataque»: conduta realizada por meio de redes, sistemas de informação ou dispositivos digitais, com o objectivo de comprometer a confidencialidade, integridade, autenticidade ou disponibilidade de dados, serviços e infra-estruturas, podendo incluir espionagem, sabotagem, roubo de informações, extorsão ou interrupção de serviços;
- f) «Ciberespaço»: ambiente digital resultante da interconexão de redes de comunicação, sistemas de informação e infra-estruturas tecnológicas, incluindo a internet, redes privadas e infra-estruturas críticas, no qual ocorrem a criação, armazenamento, processamento e transmissão de dados e informações;

- g) «Cibersegurança»: conjunto de medidas, tecnologias, políticas e práticas destinadas à protecção de redes, sistemas informáticos, infra-estruturas digitais e dados contra ameaças e ataques cibernéticos, acesso não autorizado e falhas operacionais, garantindo a confidencialidade, integridade, autenticidade e disponibilidade das informações no ambiente digital;
- h) «Comunicações Electrónicas»: informação trocada ou enviada entre um número finito de partes, mediante a utilização de um serviço de comunicações electrónicas acessíveis ao público;
- i) «CSIRT (Computer Security Incident Response Team)»: equipa de especialistas responsáveis por prevenir, gerir e responder a ameaças e ataques cibernéticos;
- j) «Dados»: representação de factos, vídeos ou imagens, informações ou conceitos, incluindo de programas de computador, que são armazenados, transmitidos ou processados num sistema de informação;
- k) «Dados Informáticos»: representação de factos, informações ou conceitos numa forma adequada para o processamento informático, incluindo um programa que permita a um sistema informático executar uma função;
- l) «Dispositivo»: equipamento, material electromagnético, acústico, mecânico, técnico ou outro programa de computador;
- m) «DNS (Domain Name System)»: sistema hierárquico e distribuído de gestão de nomes para computadores, que converte nomes de sites legíveis em endereços I.P numéricos;
- n) «DNSSEC (Domain Name System Security)»: conjunto de extensões de protocolo DNS que adiciona assinaturas digitais criptográficas aos registos de um domínio;
- o) «Funções Vitais da Sociedade»: actividades essenciais sem as quais uma sociedade moderna não consegue funcionar de forma segura e sustentável;
- p) «Incidente Informático»: qualquer evento real ou suspeito relacionado com a segurança de sistema informático ou de rede;
- q) «Infra-Estruturas Críticas»: instalação, rede, sistema, activo, serviço ou conjunto de activos físicos ou digitais, situado em território nacional, cuja disponibilidade, integridade ou funcionamento é essencial para a manutenção de funções vitais da sociedade, da segurança nacional, da saúde pública, da economia ou do bem-estar da população, e cuja perturbação, comprometimento ou destruição seja susceptível de causar um impacto grave na continuidade desses serviços ou funções, nos termos da legislação aplicável;
- r) «IMEI (International Mobile Equipment Identity)»: código pré-gravado nos equipamentos móveis, que permite a identificação do equipamento ou do terminal a nível internacional ao interligar-se a uma rede de comunicações electrónicas acessíveis ao público, considerando-se, quando aplicável, o código equivalente da tecnologia utilizada;
- s) «Operadores de Comunicações Electrónicas»: organismos, pessoas colectivas de direito público, pessoas singulares ou colectivas de direito privado ou misto, que oferecem redes ou serviços de comunicações electrónicas;
- t) «Operadores de Comunicações Electrónicas Acessíveis ao Público»: operadores de redes de comunicações electrónicas públicas e os operadores de serviços de comunicações electrónicas públicos, conforme estes sejam definidos na legislação relevante vigente;
- u) «Operador de Infra-Estruturas Críticas»: pessoa singular ou colectiva, pública ou privada, responsável pela gestão, exploração, manutenção ou controlo de uma ou mais infra-estruturas críticas, nos termos da presente Lei ou de legislação específica;
- v) «Prestador de Serviço»: pessoa singular ou colectiva, pública ou privada que, no exercício da sua actividade, disponibiliza, explora ou assegura a prestação de serviços

previstos na presente Lei, recorrendo a redes de comunicação e sistema de informação;

w) «Prestador de Serviços de Centro de Dados»: entidade, pública ou privada que presta serviços de armazenamento, tratamento e transmissão de dados, englobando estruturas ou grupos de estruturas dedicados ao alojamento, à interligação e à operação centralizada de equipamento de redes de comunicação de dados e tecnologias de informação;

x) «Prestador de Serviços de Cibersegurança»: pessoa singular ou colectiva, pública ou privada, licenciada para a prestação de serviços de cibersegurança, relacionados com o tratamento de incidentes, gestão de vulnerabilidades, teste de penetração, serviços forenses digitais, governação de cibersegurança, gestão do risco, conformidade, formação e outros serviços de cibersegurança;

y) «Prestador de Serviços de Computação em Nuvem»: pessoa singular ou colectiva, pública ou privada, que fornece, directa ou indirectamente, um conjunto de recursos flexíveis e escaláveis físicos ou virtualmente partilháveis;

z) «Prestador de Serviços de Comunicações Electrónicas»: entidade pública ou privada que presta ou explora serviços de transmissão e troca de comunicações, de forma síncrona ou assíncrona, por texto, voz, vídeo, imagem, documentos ou outros conteúdos digitais, através de redes de comunicações;

aa) «Prestador de Serviços Digitais»: pessoa singular ou colectiva, pública ou privada, prestadora de aplicações de internet que exploram, profissionalmente e com fins económicos e sociais, as plataformas digitais;

bb) «Prestador de Serviços Essenciais»: Pessoa singular ou colectiva, pública ou privada que presta serviços indispensáveis ao funcionamento da sociedade e da economia, cuja interrupção ou perturbação significativa causa um impacto relevante na continuidade de funções sociais ou económicas fundamentais;

cc) «Programa de Computador»: conjunto de instruções (software) usado directa ou indirectamente num computador, tendo em vista à obtenção de determinado resultado, incluindo o material de concepção;

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

ee) «Rede do Ciberespaço»: sistemas de transmissão ou 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 radiodifusão sonora e televisiva por cabo, independentemente do tipo de informação transmitida;

ff) «Sistema de Comunicações Electrónicas»: 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;

gg) «Sistema de Informação»: 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;

hh) «Sistema Informático»: dispositivo ou conjunto de dispositivos que procedem ao armazenamento, tratamento, recuperação ou transmissão de dados informáticos em execução de um programa de computador;

ii) «Utilizador»: pessoa com credenciais e direitos de acesso a uma rede, dispositivo ou sistema de informação.

Artigo 8.º
(Princípios fundamentais)

Na interpretação e aplicação da presente Lei, observam-se, dentre outros, os seguintes princípios:

- a) Legalidade;
- b) Proporcionalidade;
- c) Adequação;
- d) Necessidade;
- e) Protecção de dados pessoais;
- f) Tutela jurisdicional efectiva;
- g) Cooperação nacional e internacional em matéria de cibersegurança.

Capítulo II, Sistema Nacional da Cibersegurança

Secção I, Sistema Nacional da Cibersegurança

Artigo 9.º
(Composição)

O Sistema Nacional de Cibersegurança é integrado por órgãos, serviços e estratégia que concorrem para a materialização do previsto no objecto da presente Lei.

Artigo 10.º
(Órgãos)

1. São órgãos do Sistema Nacional de Cibersegurança os seguintes:
 - a) Conselho Nacional de Cibersegurança;
 - b) Centro Nacional de Cibersegurança;
 - c) Rede Nacional de CSIRT.
2. A organização, funcionamento e atribuições dos órgãos referidos no número anterior são definidos por acto normativo do Presidente da República.

Artigo 11.º
(Tipos de serviços)

1. Os serviços inerentes ao Sistema Nacional de Cibersegurança são os seguintes:
 - a) Serviços de infra-estruturas críticas e essenciais;
 - b) Serviços digitais;
 - c) Serviços de centro de dados;
 - d) Serviços de computação em nuvem;
 - e) Serviços de cibersegurança;
 - f) Serviços de comunicação electrónica;
 - g) Outros definidos por lei.
2. A natureza dos serviços referidos no número anterior, bem como a definição e obrigações dos respectivos prestadores de serviços são as estabelecidas na presente Lei.

Artigo 12.º
(Estratégia Nacional de Cibersegurança)

A Estratégia Nacional de Cibersegurança é definida por acto do Presidente da República.

Secção II, Serviços

Subsecção I, Serviços essenciais

Artigo 13.º

(Natureza dos serviços essenciais)

Os serviços essenciais constituem-se em infra-estruturas críticas cuja disponibilidade, integridade, autenticidade e confidencialidade são indispensáveis para a manutenção de funções vitais da sociedade, da segurança nacional, da saúde pública, da economia ou do bem-estar da população.

Artigo 14.º

(Obrigações do operador de infra-estruturas críticas e de serviços essenciais)

1. São obrigações do operador de infra-estruturas críticas as seguintes:

- a) Estabelecer CSIRT institucional;
- b) Designar ponto focal de cibersegurança;
- c) Aderir a CSIRT sectorial, de acordo com a dimensão, risco e criticidade da entidade;
- d) Implementar medidas técnico-organizativas adequadas e proporcionais aos riscos identificados, em conformidade com os requisitos mínimos de segurança estabelecidos na presente Lei;
- e) Adoptar uma abordagem de gestão de riscos para identificar, compreender e mitigar os riscos para prevenir incidentes cibernéticos;
- f) Dispor de procedimentos sólidos para recuperação célere de incidentes cibernéticos;
- g) Manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados, nos termos da Lei de Protecção de Dados;
- h) Preservar e fornecer dados ou informações às autoridades competentes nos casos, termos, limites e garantias previstos na Constituição e na lei;
- i) Informar ao CERT.ao sobre ciberameaças e ciberataques que registem na sua actividade;
- j) Implementar processos internos de gestão da cibersegurança, com objectivos, responsabilidades e mecanismos de monitorização adequados aos riscos identificados;
- k) Promover formação e capacitação periódica em matéria de cibersegurança e documentar as decisões relevantes.

2. São obrigações do operador de serviços essenciais as seguintes:

- a) Realizar avaliação sistemática do risco de ocorrência de incidentes e gerir o mesmo;
- 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. Continuidade da prestação dos serviços essenciais, mesmo em caso de incidente de cibersegurança;
 - 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) Recolher informações sobre ciberameaças e vulnerabilidades do sistema de informação utilizado para prestar o serviço essencial;
 - d) 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. Gestão segura e tempestiva das actualizações de software;
 - iii. Protecção contra modificações não autorizadas no sistema de informação;
 - iv. Tomada de medidas imediatas e proporcionais quando forem identificadas vulnerabilidades ou ciberameaças.
 - e) Utilizar meios de comunicação que permitam uma comunicação adequada e segura no âmbito do sistema nacional de cibersegurança;
 - f) Adoptar políticas de cópias de segurança, recuperação de desastres, continuidade de negócio, gestão de crises, segurança da cadeia de fornecimento, controlo de acessos, autenticação multifactor e criptografia adequada ao risco;
 - g) Designar responsável pela cibersegurança e assegurar que o órgão de gestão aprove e acompanhe as medidas de gestão de risco.
3. Para o exercício das suas actividades, o operador de infra-estruturas críticas e de serviços essenciais deve registar-se no Centro Nacional de Cibersegurança.

Subsecção II, Serviços digitais

Artigo 15.º

(Natureza dos serviços digitais)

Os serviços digitais constituem-se em aplicações da internet em que se explora, profissionalmente e com fins económicos e sociais, as plataformas digitais.

Artigo 16.º

(Obrigações do prestador de serviços digitais)

1. São obrigações do prestador de serviços digitais as seguintes:
- a) Conservar os registos técnicos, contratuais e de segurança estritamente necessários, adequados e proporcionais à prestação do serviço, à prevenção de incidentes e ao cumprimento de obrigações legais, observados os princípios de finalidade, minimização e prazo de conservação;
 - b) Estabelecer CSIRT institucional, designar ponto focal de cibersegurança ou aderir a CSIRT sectorial, em função da dimensão, risco e criticidade da actividade;
 - 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) Implementar as normas técnicas adequadas para protecção de redes e sistemas informáticos;
 - f) Garantir a segurança dos dados armazenados em ambientes de computação em nuvem;
 - g) Notificar incidentes de cibersegurança ao CERT.ao e ao CSIRT sectorial competente nos prazos previstos na presente Lei e nos regulamentos técnicos aplicáveis, sem prejuízo de notificação à autoridade de protecção de dados pessoais quando estejam em causa dados pessoais;

- h) Manter sigilo sobre as comunicações e informações transmitidas ou tratadas pelos utilizadores e clientes, salvo nos casos e termos previstos na Constituição e na lei.
2. Para o exercício das suas actividades, o operador de serviços digitais deve registar-se no Centro Nacional de Cibersegurança.
3. O prestador de Serviços digitais que presta serviços ao Estado está sujeito a regulamentação específica.
4. O dever de identificação ou registo de utilizadores não pode ser interpretado como obrigação geral de identificação civil de todos os utilizadores de Serviços digitais, nem como autorização para recolha massiva de dados pessoais ou de conteúdo das comunicações.

Subsecção III, Serviços de centros de dados

Artigo 17.º

(Natureza dos serviços de centros de dados)

Os serviços de centros de dados constituem-se em infra-estruturas tecnológicas destinadas ao armazenamento, tratamento e transmissão de dados, que engloba estruturas ou grupos de estruturas dedicados ao alojamento, à interligação e à operação centralizadas de redes de comunicação de dados e tecnologias da informação.

Artigo 18.º

(Obrigações do prestador de serviços de centro de dados)

1. São obrigações do prestador de serviços de centro de dados as seguintes:
- a) Adoptar medidas de identificação e autenticação proporcionais ao risco, bem como de conservação dos registos técnicos, contratuais e de segurança estritamente necessários e adequados à prestação do serviço, à prevenção de incidentes e ao cumprimento de obrigações legais, observados os princípios da protecção de dados pessoais, da finalidade e da limitação do prazo de conservação;
 - b) Estabelecer o CSIRT institucional;
 - c) Garantir que os dados conservados sejam da mesma qualidade e sujeitos à 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 registados na sua actividade;
 - f) Contratar e manter em vigor seguro adequado à cobertura dos riscos decorrentes da prestação dos seus serviços;
 - g) 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, o prestador de serviços de centros de dados deve registar-se no Centro Nacional de Cibersegurança.
3. O prestador de serviços de centros de dados que presta serviços ao Estado está sujeito à regulamentação específica.

Subsecção IV, Serviços de computação em nuvem

Artigo 19.º

(Natureza dos serviços de computação em nuvem)

Os serviços de computação em nuvem constituem-se no conjunto de recursos flexíveis e escaláveis físico ou virtualmente compartilháveis.

Artigo 20.º

(Obrigações do prestador de serviços de computação em nuvem)

1. São obrigações do prestador de serviços de computação em nuvem as seguintes:
 - a) Estabelecer o CSIRT institucional;
 - b) Registar os seus utilizadores;
 - c) Garantir que os dados conservados sejam da mesma qualidade e sujeitos à 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 registados 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, o prestador de serviços de computação em nuvem deve registar-se no Centro Nacional de Cibersegurança.
3. O prestador de serviços de computação em nuvem privada que presta serviços ao Estado está sujeito à regulamentação específica.

Subsecção V, Serviços de cibersegurança

Artigo 21.º

(Natureza do serviço de cibersegurança)

O serviço de cibersegurança constitui-se em dispositivos de monitorização, controlo, gerenciamento, avaliação de riscos e recuperação de incidentes cibernéticos.

Artigo 22.º

(Obrigações do prestador de serviços de cibersegurança)

1. São obrigações do prestador de serviços de cibersegurança as seguintes:
 - a) Descrever os serviços oferecidos e os processos técnicos envolvidos;
 - b) Manter em sigilo todas as comunicações de informação transmitidas pelos utilizadores a si vinculados;
 - c) Adoptar medidas técnicas e organizacionais necessárias à antecipação, detecção, reacção e recuperação dos danos causados por incidentes cibernéticos;
 - d) Informar ao CERT.ao sobre ciberameaças e ciberataques registados na sua actividade;
 - 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, o prestador de serviços de cibersegurança deve registar-se no Centro Nacional de Cibersegurança.

Subsecção VI, Serviços de comunicações electrónicas

Artigo 23.º

(Natureza dos serviços de comunicações electrónicas)

Os serviços de comunicações electrónicas constituem-se em redes de telecomunicações para transmissão de sinais por texto, voz, vídeo, imagem ou documento.

Artigo 24.º

(Obrigações do prestador de serviços de comunicações electrónicas)

1. São obrigações do prestador de serviços de comunicações electrónicas as seguintes:
 - a) Registar os seus utilizadores;
 - b) Estabelecer o CSIRT institucional;
 - c) Garantir que os dados conservados sejam da mesma qualidade e sujeitos à 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 registados 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, o prestador de serviços de comunicações electrónicas deve registar-se no Centro Nacional de Cibersegurança.

Capítulo III, Segurança das redes e dos sistemas de informação

Secção I, Segurança das redes e dos sistemas de informação

Artigo 25.º

(Segurança de redes de comunicação de dados)

As redes do ciberespaço devem assegurar a integridade, disponibilidade, autenticidade, confidencialidade e protecção das comunicações, mediante a implementação de medidas técnicas e organizativas adequadas ao risco, incluindo gestão de acessos, monitorização de segurança, gestão de vulnerabilidades, actualizações, cópias de segurança, criptografia, continuidade de serviço e resposta a incidentes.

Artigo 26.º

(Segurança na utilização da internet)

1. As entidades que prestam serviços de comunicação de dados através de redes de internet devem adoptar medidas técnicas e organizativas adequadas para garantir a integridade, confidencialidade e segurança das informações transmitidas, bem como a protecção dos sistemas de informação envolvidos.
2. As medidas previstas no número anterior devem basear-se em normas técnicas internacionalmente reconhecidas e boas práticas de cibersegurança, sem prejuízo da legislação nacional aplicável.
3. A implementação das medidas de segurança deve assegurar a protecção contra acessos não autorizados, alterações indevidas, perda de dados e outras ameaças à segurança das comunicações.

Artigo 27.º

(Protecção do sistema de nomes de domínio)

Os gestores de domínios, registos de nomes de domínio e entidades tecnicamente responsáveis pelo sistema de nomes de domínio (DNS) devem adoptar medidas proporcionais para assegurar a sua disponibilidade, integridade, autenticidade e resiliência,

incluindo a implementação faseada de segurança de nomes de domínio (DNSSEC), sempre que tecnicamente viável, bem como procedimentos de verificação, correcção e acesso lícito a dados de registo de domínio, em conformidade com a Lei de Protecção de Dados Pessoais.

Secção II, Requisitos de segurança e notificação de incidentes

Artigo 28.º

(Incidentes de cibersegurança de impacto significativo)

1. Considera-se que um incidente de cibersegurança tem impacto significativo quando, em função da avaliação objectiva do risco e do impacto, preencha pelo menos uma das seguintes condições:

- a) Cause ou possa causar perturbação operacional grave, perda financeira relevante, indisponibilidade prolongada ou redução substancial da qualidade do serviço;
- b) Afecte ou possa afectar um número relevante de utilizadores, destinatários de serviços, cidadãos, empresas, entidades públicas ou serviços dependentes;
- c) Tenha ou possa ter impacto transfronteiriço, intersectorial ou sistémico;
- d) Envolver violação de dados pessoais, segredo das comunicações, dados sensíveis, informação classificada ou informação protegida por dever legal de sigilo profissional ou confidencialidade;
- e) Exija medidas excepcionais de recuperação, contenção, continuidade de negócio, gestão de crise ou comunicação pública para proteger a segurança das redes, dos sistemas de informação ou dos destinatários dos serviços.

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

Artigo 29.º

(Requisitos de segurança e normalização)

1. Os requisitos de segurança aplicáveis à segurança das redes e dos sistemas de informação são definidos de modo a assegurar a confidencialidade, integridade, autenticidade, disponibilidade, segurança e resiliência das redes e sistemas de informação, interoperabilidade, utilização de normas técnicas internacionalmente reconhecidas e a neutralidade tecnológica, sem imposição ou discriminação de soluções ou fornecedores específicos.

2. Os requisitos de segurança incluem, designadamente, medidas de prevenção, detecção, resposta e recuperação de ataques ou incidentes, bem como mecanismos de gestão de risco e de continuidade de serviços.

3. A especificação técnica detalhada dos requisitos referidos nos números anteriores é definida em regulamentos.

Artigo 30.º

(Requisitos de notificação de incidentes)

1. As entidades abrangidas pela obrigação de notificação de incidentes de cibersegurança devem comunicar às entidades competentes qualquer incidente que tenha impacto significativo na continuidade, segurança ou integridade das redes e sistemas de informação sob sua responsabilidade.

2. Para efeitos do disposto no número anterior, consideram-se sujeitas à obrigação de notificação, designadamente:

- a) Administração Pública;
- b) CSIRT sectoriais e CSIRT institucionais;

- c) Operadores de infra-estruturas críticas e de serviços previstos na presente Lei;
 - d) Outras entidades que utilizem redes e sistemas de informação, em função da dimensão, risco, criticidade ou impacto económico e social da actividade.
3. A notificação ao CERT.ao ou a CSIRT sectorial não substitui as notificações legalmente devidas à autoridade de protecção de dados pessoais, aos reguladores sectoriais, às autoridades judiciais ou aos destinatários dos serviços, quando aplicável.
4. A notificação de incidentes deve incluir, pelo menos:
- a) A descrição do incidente e a sua natureza;
 - b) O impacto estimado sobre os serviços afectados;
 - c) As medidas de contenção adaptadas;
 - d) A avaliação preliminar da causa do incidente;
 - e) Outras informações relevantes para a gestão da resposta.
5. A notificação deve ser efectuada no prazo a definir em diploma próprio, sem prejuízo da comunicação imediata em caso de incidentes de elevado impacto.
6. Os requisitos técnicos, procedimentais e os canais de notificação são definidos em regulamento.
7. O disposto no presente artigo não se aplica:
- a) Às redes e sistemas de informação directamente relacionados com o comando e controlo das entidades que superintendem as áreas da Defesa Nacional, Segurança e Ordem Interna sujeitas à lei própria;
 - b) Às redes e sistemas de informação que processem informação classificada conforme legislação específica.

Artigo 31.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.
4. Para efeitos da presente Lei, constituem requisitos mínimos de segurança, designadamente:
- a) A adopção de políticas e procedimentos de gestão de risco em cibersegurança;
 - b) A implementação de medidas de prevenção, detecção, resposta e recuperação de incidentes;
 - c) A protecção da disponibilidade, integridade, confidencialidade e autenticidade das redes e dos sistemas de informação;
 - d) A implementação de mecanismos de controlo de acessos e gestão de identidades;
 - e) A realização periódica de avaliações de risco e testes de segurança;
 - f) A adopção de planos de continuidade dos serviços e de recuperação em caso de incidente;

g) A promoção de acções de formação e sensibilização em matéria de cibersegurança para os seus colaboradores.

5. Os requisitos técnicos específicos para a implementação das medidas previstas no presente artigo são definidos em regulamento, tendo em conta à natureza, dimensão, nível de risco e criticidade das entidades abrangidas.

Artigo 32.º

(Notificação de incidentes pela 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 CSIRT institucionais e notificar ao respectivo CSIRT sectorial, caso exista, e ao CERT.ao os incidentes com um impacto relevante na segurança das redes e dos sistemas de informação.

2. A notificação dos operadores de infra-estruturas críticas inclui informação que permita ao CERT.ao determinar o impacto transfronteiriço dos incidentes.

3. 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.

4. Sempre que as circunstâncias o permitam, o órgão competente presta ao notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente, informações que possam contribuir para o tratamento eficaz do incidente.

5. O órgão competente pode divulgar incidentes específicos de acordo com o interesse público, salvaguardando a segurança e os interesses dos operadores de infra-estruturas críticas.

6. Os órgãos e serviços da Administração Pública e os operadores de infra-estruturas críticas devem submeter ao CSIRT sectorial e ao CERT.ao relatório final de resposta e resolução do incidente, no prazo legalmente estabelecido, sem prejuízo de relatórios intercalares quando solicitados ou quando o incidente se mantenha em curso.

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 em diploma próprio.

8. A notificação, por si só, não constitui reconhecimento de responsabilidade civil, administrativa ou criminal, nem pode ser utilizada como fundamento exclusivo para responsabilizar a entidade notificante.

Artigo 33.º

(Requisitos de segurança para os prestadores de serviços essenciais)

1. Os prestadores de serviços essenciais devem adoptar medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação utilizados na prestação dos serviços essenciais sob sua responsabilidade.

2. As medidas previstas no número anterior devem assegurar um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.

3. Os prestadores de serviços essenciais devem tomar medidas preventivas 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 34.º

(Notificação de incidentes pelos prestadores de serviços essenciais)

1. Os prestadores de serviços essenciais devem estabelecer CSIRT institucionais, quando exigido, em função da sua dimensão, criticidade e risco, e notificar o CSIRT sectorial competente e o CERT.ao os incidentes com impacto relevante na continuidade dos serviços essenciais por si prestados, no prazo legalmente estabelecido.
2. Sempre que um prestador 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.
3. A notificação inclui informação que permita ao Centro Nacional de Cibersegurança determinar o impacto transfronteiriço dos incidentes.
4. Aplica-se ao prestador de serviços essenciais, com as devidas adaptações, as regras de notificação estabelecidas para a Administração Pública.

Artigo 35.º

(Requisitos de segurança para os prestadores de serviços digitais)

1. Os prestadores de serviços digitais devem identificar e tomar 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 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 aos progressos técnicos mais recentes e devem ter em conta aos 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 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 definidos em regulamento.

Artigo 36.º

(Notificação de incidentes pelos prestadores de serviços digitais)

1. Os prestadores de serviços digitais devem notificar ao respectivo CSIRT sectorial e ao CERT.ao os incidentes com impacto relevante na continuidade dos serviços digitais por si prestados, no prazo legalmente estabelecido.
2. Aplica-se aos prestadores de serviços digitais, com as devidas adaptações, as regras de notificação estabelecidas para a Administração Pública.

Artigo 37.º

(Requisitos de segurança para prestadores de serviços de centros de dados)

1. Os prestadores de serviços 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 inatividade.
2. Os requisitos técnicos e de conformidade aplicáveis aos centros de dados são definidos em diploma próprio.

Artigo 38.º

(Notificação de incidentes pelos prestadores de serviços de centros de dados)

1. Os prestadores de serviços de centros de dados devem notificar os seus clientes sobre incidentes de cibersegurança que afectem ou possam afectar os dados, conteúdos ou serviços prestados, incluindo violação de dados pessoais, quando aplicável.
2. Os prestadores de serviços de centros de dados devem notificar ao CERT.ao, no prazo legalmente estabelecido.
3. Os prestadores de serviços de centros de dados devem notificar os seus assinantes sobre a existência, o âmbito e as condições de cobertura do seguro de responsabilidade civil por si disponibilizado.
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 prestadores de serviços 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 prestadores de centros de dados devem submeter ao CSIRT sectorial e ao CERT.ao relatório final de resposta e resolução do incidente no prazo legalmente estabelecido.
7. O relatório de resposta e resolução de incidentes inclui informações sobre as causas do incidente de cibersegurança, o tempo dedicado para a sua resolução, as medidas aplicadas, o impacto da mesma e todas as outras informações exigidas pelos regulamentos desta Lei.

Artigo 39.º

(Requisitos de segurança para prestadores de serviços de plataformas de computação em nuvem)

1. Os prestadores de serviços de computação em nuvem devem avaliar e gerir os riscos de segurança associados ao armazenamento, processamento, transferência, segregação, disponibilidade e recuperação de dados em ambientes de nuvem, assegurando configuração segura, controlo de acessos, registo técnico, continuidade de negócio, reversibilidade, portabilidade, conformidade contratual e adopção de boas práticas reconhecidas.
2. Os requisitos técnicos específicos de segurança aplicáveis às plataformas de computação em nuvem são definidos em diploma próprio, tendo em conta à natureza, dimensão e nível de risco dos serviços prestados.

Artigo 40.º

(Notificação de incidentes pelos prestadores de serviços de computação em nuvem)

Sem prejuízo do disposto na presente Lei, os prestadores de serviços de computação em nuvem devem:

- a) Notificar os seus clientes, sem atraso injustificado, sobre quaisquer incidentes de cibersegurança que afectem ou possam afectar conteúdos, dados ou serviços fornecidos, incluindo violação de dados pessoais quando aplicável;

- b) Notificarão CERT.ao, nos prazos previstos na presente Lei, qualquer incidente de cibersegurança de impacto significativo, incluindo violação de dados pessoais, sem prejuízo de notificação à autoridade de protecção de dados pessoais quando aplicável;
- c) Notificar aos assinantes de qualquer cobertura de seguro fornecida pelo serviço contra qualquer responsabilidade civil para esses assinantes, devendo incluir, pelo menos, as características básicas que possam ser razoavelmente necessárias para os assinantes avaliarem a sua exposição ao risco e tomarem decisões sobre a cobertura de seguro e conformidade;
- d) 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;
- e) Submeter ao CSIRT sectorial e ao CERT.ao relatório final sobre a resposta e resolução do incidente no prazo legalmente estabelecido.

Artigo 41.º

(Requisitos de segurança e notificação aplicáveis aos prestadores de serviços de cibersegurança)

1. Aplica-se aos prestadores de serviços de cibersegurança, com as devidas adaptações, as regras de segurança e de notificação estabelecidas para a Administração Pública, nos termos da presente Lei.
2. Os requisitos técnicos e de conformidade aplicáveis aos serviços de cibersegurança são definidos em regulamento.

Artigo 42.º

(Requisitos de segurança e notificação aplicáveis aos prestadores de serviços de comunicações electrónicas)

1. Aplica-se aos Prestadores de Comunicações Electrónicas, com as devidas adaptações, as regras de segurança e de notificação estabelecidas para a Administração Pública, nos termos da presente Lei.
2. Os requisitos técnicos e de conformidade aplicáveis aos serviços de comunicações electrónicas são definidos em regulamento.

Artigo 43.º

(Notificação voluntária de incidentes)

1. Sem prejuízo da obrigação de notificação de incidentes prevista na presente Lei, qualquer entidade pode notificar ao CSIRT sectorial, CSIRT institucional ou CERT.ao, a título voluntário, os incidentes com impacto importante na prevenção, detecção, resposta, recuperação e mitigação de incidentes de cibersegurança por si prestados.
2. A notificação voluntária inviabiliza a imposição à entidade notificante a eventuais obrigações decorrentes dessa notificação.
3. As informações recebidas no âmbito de notificação voluntária são protegidas por dever de confidencialidade e só podem ser partilhadas com outras autoridades, quando tal seja necessário, proporcional e legalmente admissível para prevenir, conter ou responder a incidentes.

Capítulo IV, Resposta a ameaças e incidentes de cibersegurança

Artigo 44.º

(Acções para prevenir e gerir incidentes de cibersegurança)

Sempre que o CERT.ao receber informações ou tomar conhecimento sobre ciberameaças ou incidentes de cibersegurança de impacto significativo, deve notificar a entidade afectada, o órgão regulador sectorial competente e o CSIRT sectorial correspondente, para que, no exercício das respectivas competências e com respeito pelos princípios da celeridade, necessidade, proporcionalidade, menor intrusão, coordenação institucional e continuidade dos serviços, sejam realizadas as acções necessárias para prevenir, conter, gerir e recuperar da ameaça ou incidente de cibersegurança em infra-estruturas críticas ou serviços essenciais, visando:

- a) Avaliar o impacto ou potencial impacto da ameaça ou incidente;
- b) Eliminar ou conter a ciberameaça e prevenir danos adicionais resultantes do incidente de cibersegurança;
- c) Impedir que um novo incidente de cibersegurança surja como consequência da ocorrência anterior.

Artigo 45.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 deve notificar o CERT.ao, no prazo legalmente definido, para efeitos de correlação técnica com outros incidentes relevantes reportados por sectores de infra-estruturas críticas ou serviços essenciais.

Artigo 46.º

(Medidas de prevenção e gestão de incidentes)

Para prevenir e gerir incidentes de cibersegurança, o CERT.ao ou o CSIRT sectorial, mediante decisão fundamentada e proporcional, deve adoptar as seguintes medidas:

- a) Exigir ao operador de infra-estrutura crítica que informe sobre qualquer incidente de cibersegurança de impacto significativo que o afecte ou tenha afectado;
- b) Exigir ao operador de infra-estrutura crítica ou ao operador de sistema de informação que realize medidas preventivas ou correctivas para responder ao incidente, nos termos da presente Lei e dos regulamentos aplicáveis;
- c) Solicitar ao operador de sistema de informação ligado ao operador de infra-estrutura crítica que realize acções tecnicamente necessárias para apoiar a gestão do incidente de cibersegurança, incluindo:
 - i. Preservar o estado do sistema de informação e os registos técnicos necessários à resposta ao incidente;
 - ii. Realizar análise do sistema de informação para detectar vulnerabilidades de cibersegurança e avaliar o modo e a amplitude em que o sistema foi afectado pelo incidente de cibersegurança.

Artigo 47.º

(Entrega de informações)

1. As entidades públicas e privadas abrangidas pela presente Lei devem facultar ao CSIRT institucional, ao CSIRT sectorial ou ao CERT.ao as informações técnicas e operacionais necessárias à prevenção, detecção, análise e resposta a incidentes de cibersegurança, incluindo dados de registos, indicadores de comprometimento, descrições de incidentes e medidas de mitigação adaptadas.

2. A transmissão das informações referidas no número anterior não constitui violação de dever de confidencialidade previsto em lei, regulamento, contrato ou código de conduta profissional, constituindo uma obrigação legal de cooperação em matéria de cibersegurança, sem prejuízo do respeito pela protecção de dados pessoais.
3. As informações entregues ao CSIRT sectorial ou ao CERT.ao são reservadas e confidenciais, devendo ser protegidas contra acesso indevido, divulgação não autorizada e utilização para finalidades alheias à prevenção, resposta, recuperação, fiscalização ou procedimento legalmente competente.
4. Caso o sistema de informação esteja comprometido por ciberataque ou incidente iminente susceptível de o prejudicar ou destruir significativamente, o CSIRT sectorial ou o CERT.ao pode recomendar ou determinar, quando legalmente competente e de modo proporcional, a limitação temporária do uso do sistema ou de componentes estritamente necessários, devendo a decisão ser fundamentada, registada e comunicada ao operador, sem prejuízo das garantias legalmente previstas.
5. As medidas previstas no número anterior não podem abranger, sem autorização judicial, o acesso ao conteúdo de comunicações privadas, a dados pessoais não indispensáveis à gestão do incidente ou a dados protegidos por segredo profissional, salvo nos casos expressamente previstos na lei.
6. Para o cumprimento do previsto no presente artigo, é assegurada a existência da Rede Nacional de CSIRT, que se constitui num fórum de partilha de informação de carácter operacional sobre incidentes cibernéticos entre o CERT.ao, os CSIRT sectoriais e institucionais, nos termos a definir em regulamento.

Artigo 48.º

(Comunicação responsável de vulnerabilidades)

1. Qualquer pessoa, singular ou colectiva, pode comunicar, de boa-fé, vulnerabilidades aos órgãos legalmente competentes em matéria de cibersegurança, 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 comunicado tais informações.
2. Para efeitos da presente Lei, considera-se que a comunicação de uma vulnerabilidade é de boa-fé, quando:
 - a) Não tiver sido feita sob coação, ameaça de comunicação de informações ou exigência indevida de recompensa, sem prejuízo de recompensa previamente prevista em programa autorizado de comunicação de vulnerabilidades;
 - b) 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;
 - c) A pessoa que comunica uma vulnerabilidade considera o impacto de tal comunicação e toma os devidos cuidados para minimizar o dano que pode ser causado.
3. A partir do processo de identificação de vulnerabilidades baseado na boa-fé, são excluídos os métodos que possam levar a:
 - a) Negação de serviço;
 - b) Intrusão física, acesso não autorizado a instalações ou superação de barreiras físicas;
 - c) Uso de código malicioso, engenharia social, acesso indevido a dados de terceiros ou exfiltração de informação;
 - d) Alteração, remoção, destruição, comunicação ou cópia não autorizada de dados.

4. A entidade receptora da comunicação de vulnerabilidade deve acusar a recepção no prazo legalmente estabelecido, indicar ponto de contacto e cooperar de boa-fé com o comunicante, sem prejuízo da protecção de segredos comerciais, dados pessoais e segurança pública.

Artigo 49.º **(Salvaguarda de competências)**

A adopção das medidas previstas nos artigos anteriores não prejudica as competências das autoridades judiciais, das autoridades de investigação criminal e das demais entidades legalmente competentes.

Capítulo V, Supervisão, fiscalização e auditoria

Artigo 50.º **(Supervisão)**

O órgão regulador da cibersegurança garante a supervisão dos serviços previstos na presente Lei, em articulação com os reguladores sectoriais competentes e com respeito pela legalidade, proporcionalidade, protecção de dados pessoais, segredo comercial, segredo profissional e informação classificada, nos termos a definir em diploma próprio.

Artigo 51.º **(Fiscalização)**

O órgão regulador da cibersegurança realiza acções de fiscalização das redes e sistemas informáticos, com vista a garantir a qualidade dos serviços e a integridade da cibersegurança, salvaguardando os dados pessoais, os segredos legalmente protegidos e a continuidade de serviços essenciais, nos termos a definir em regulamento.

Artigo 52.º **(Auditoria)**

O órgão regulador da cibersegurança ordena auditorias de cibersegurança no âmbito do processo contra-ordenacional, devendo observar-se os padrões técnicos aceitáveis, sem prejuízo da realização de auditorias independentes equivalentes, nos termos a definir em diploma próprio.

Capítulo VI, Responsabilidade

Secção I, Responsabilidade civil e criminal

Artigo 53.º **(Responsabilização)**

1. A responsabilidade civil emergente da violação do disposto na presente Lei é regulada nos termos gerais do Direito.
2. A responsabilidade penal emergente da violação do disposto na presente Lei rege-se pelo Código Penal e pela demais legislação aplicável.

Secção II, Regime contra-ordenacional

Artigo 54.º

(Contra-ordenações)

Constituem contra-ordenações as infracções de natureza administrativa ao disposto na presente Lei.

Artigo 55.º

(Espécies de contra-ordenações)

1. Constituem contra-ordenações leves a submissão de relatórios periódicos fora do prazo legalmente estabelecido.
2. Constituem contra-ordenações graves:
 - a) Falta de registo necessário ao exercício da actividade;
 - b) Falta de notificação de incidentes ao CERT.ao, no prazo legalmente definido;
 - c) Não submissão de relatórios periódicos definidos pela presente Lei;
 - d) Falta de elaboração ou manutenção do plano de resposta a incidentes, nos casos como tal exigidos;
 - e) Não cumprimento dos regulamentos técnicos e metodológicos emitidos pelo órgão legalmente competente;
 - f) Não cumprimento dos requisitos de segurança por parte dos fornecedores de tecnologia e serviços com os seus clientes.
3. Constituem contra-ordenações muito graves:
 - a) Incumprimento da obrigação de implementar os requisitos de segurança tal como previstos na presente Lei;
 - b) Omissão ou falsificação de informações nos relatórios de auditoria ou gestão de riscos, tal como previstos na presente Lei;
 - c) Obstrução dolosa de supervisão, fiscalização ou auditoria legitimamente ordenada;
 - d) Divulgação não autorizada de informação confidencial recebida no âmbito de notificação, fiscalização, auditoria ou resposta a incidentes;
 - e) Incumprimento doloso de ordem técnica urgente, fundamentada e proporcional, destinada a prevenir ou conter incidente de impacto significativo.

Artigo 56.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 seu impacto na segurança das redes e sistemas de informação, bem como da condição económica do agente.
2. O valor da coima para as contra-ordenações leves é fixado da seguinte forma:
 - a) Para pessoas singulares, o montante mínimo é de 7 salários mínimos nacionais e o máximo de 70 salários mínimos nacionais;
 - b) Para pessoas colectivas, o montante mínimo é de 70 salários mínimos nacionais e o máximo de 150 salários mínimos nacionais.
3. O valor da coima para as contra-ordenações graves é fixado da seguinte forma:
 - a) Para pessoas singulares, o montante mínimo é de 100 salários mínimos nacionais e o máximo de 250 salários mínimos nacionais;
 - b) Para pessoas colectivas, o montante mínimo é de 300 salários mínimos nacionais e o máximo de 500 salários mínimos nacionais.

4. O valor da coima para as contra-ordenações muito graves é fixado da seguinte forma:
- a) Para pessoas singulares, o montante mínimo é de 150 salários mínimos nacionais e o máximo de 450 salários mínimos nacionais;
 - b) Para pessoas colectivas, o montante mínimo é de 2.000 salários mínimos nacionais e o máximo de 4.000 salários mínimos nacionais.
5. As coimas aplicáveis por contra-ordenações à presente Lei devem ser pagas no prazo máximo de 30 dias, contados a partir da data de notificação da decisão que as aplicou.

Artigo 57.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 com os requisitos estabelecidos, em caso de reincidência ou contra-ordenações graves;
- b) Proibição de participação em procedimentos de contratação pública relacionados com o respectivo sector de actividade, por um período não superior a 3 (três) anos, em caso de contra-ordenação muito grave e reiterada.

Artigo 58.º **(Competências para a fiscalização e aplicação de sanções)**

As competências de fiscalização e de aplicação das sanções administrativas previstas na presente Lei cabem ao Centro Nacional de Cibersegurança.

Artigo 59.º **(Registo da decisão)**

1. O órgão competente para aplicar as coimas e as sanções acessórias deve proceder ao registo da decisão que as mande aplicar, nos termos da presente Lei.
2. O registo previsto no número anterior destina-se exclusivamente ao exercício das competências legais de fiscalização, controlo de reincidência, execução das decisões e tratamento estatístico institucional.

Artigo 60.º **(Publicidade da decisão)**

1. A decisão definitiva que aplicar coima e sanção acessória por contra-ordenação grave ou muito grave pode ser objecto de publicidade, quando tal se revele necessário para:
 - a) Protecção do interesse público;
 - b) Prevenção de novas infracções;
 - c) Salvaguarda da confiança e segurança no ambiente digital.
2. A publicidade da decisão é determinada pela entidade competente e deve limitar-se ao estritamente necessário, observando as garantias decorrentes da protecção de dados pessoais e empresariais.
3. A publicidade pode ser efectuada através das páginas na internet e das entidades públicas do sector de actividade em que actua o infractor, sem prejuízo da divulgação nos canais de comunicação social públicos.

Artigo 61.º **(Processo contra-ordenacional)**

O processo contra-ordenacional deve, dentre outros, observar os princípios do contraditório e da ampla defesa, nos termos da lei.

Artigo 62.º
(Direito subsidiário)

Em tudo quanto não estiver especialmente regulado na presente Lei, em matéria contra-ordenacional, aplica-se subsidiariamente o disposto na Lei sobre o Regime Geral das Contra-Ordenações.

Capítulo VII, Disposições finais e transitórias

Artigo 63.º
(Regime subsidiário)

Em tudo o que não contrarie o disposto na presente Lei, aplicam-se supletiva e subsidiariamente os seguintes diplomas legais:

- a) Lei da Protecção de Dados Pessoais;
- b) Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação;
- c) Lei sobre o Regime Geral das Contra-Ordenações;
- d) Código de Processo do Contencioso Administrativo;
- e) Código Penal;
- f) Código do Processo Penal;
- g) Normas constantes de tratados e convenções internacionais.

Artigo 64.º
(Regime transitório)

As entidades sujeitas a registo, ao abrigo desta Lei, devem proceder ao respectivo registo no prazo de 180 dias, a contar da data de entrada em vigor da presente Lei.

Artigo 65.º
(Revogação)

É revogada a Lei n.º 7/17, de 16 de Fevereiro, Lei de Protecção das Redes e Sistemas Informáticos, bem como todas as disposições legais que contrariem o disposto na presente Lei.

Artigo 66.º
(Dúvidas e omissões)

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

Artigo 67.º
(Entrada em vigor)

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

Vista e aprovada pela Assembleia Nacional, em Luanda, aos 12 de Agosto de 2026.

O Presidente da Assembleia Nacional, Adão Francisco Correia de Almeida.

Promulgada aos 8 de Setembro de 2026. Publique-se.

O Presidente da República, João Manuel Gonçalves Lourenço.