Proposta de Lei
Versão 2.0
07/03/2023

República de Moçambique
Assembleia da República

Lei nº /2022

De de

Havendo necessidade de estabelecer o regime jurídico da Segurança Cibernética que visa responder de forma eficaz e eficiente aos novos desafios da Sociedade da Informação, bem como garantir a segurança do cidadão, sistemas de informação e infraestruturas críticas, no espaço cibernético ao abrigo do disposto do n.º 1 do artigo 178, da Constituição da República à Assembleia da República determina:

CAPÍTULO I

Disposições Gerais

Artigo 1

(Objecto)

A presente Lei estabelece o regime jurídico da Segurança Cibernética, visando garantir a segurança do cidadão e instituições, bem como assegurar a protecção de redes, sistemas de informação e infraestruturas críticas no espaço cibernético.

Artigo 2

(Âmbito)

1. A presente lei aplica-se à rede de qualquer pessoa singular, colectiva pública ou privada, nos domínios dos provedores intermediários de serviços e dos provedores de serviços digitais com destaque para os seguintes:
   a) Operador de rede de infraestruturas críticas;
   b) Operador de rede de serviços essenciais;
   c) outras entidades que utilizam redes e sistemas de informação.

2. Exceptuan-se do previsto no n.º 1 do presente artigo, as seguintes redes:

   a) 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) redes e sistemas de informação que processem informação classificada conforme a legislação específica.

3. Caso uma entidade se enquadre simultaneamente em mais de uma das alíneas constantes no n.º 1 do presente artigo, aplica-se o regime que resultar mais exigente para a segurança das redes e dos sistemas de informação.

Artigo 3

(Definições)

Para efeitos da presente lei, as definições dos termos e acrónimos constam no glossário em anexo, o qual é parte integrante da mesma.

Artigo 4

(Princípios)

A presente lei rege-se pelos seguintes princípios:

a) Colaboração: consiste na implementação de medidas para assegurar a estabilidade, aumentar segurança e evitar práticas consideradas prejudiciais ou susceptíveis de pôr em perigo o uso das Tecnologias de Informação e Comunicação (TIC);

b) Cooperação: consiste na troca de informações, assistência mútua, entre Estados, no âmbito de ameaças e incidentes de segurança cibernética;

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

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

e) Transparência: o Estado deve assegurar a não proliferação de inovações, técnicas e instrumentos maliciosos, bem como o uso de funções ocultas e prejudiciais no domínio das TIC;

f) Divulgação de vulnerabilidades: encorajar a divulgação responsável de vulnerabilidades de segurança cibernética.

Artigo 5

(Política de Segurança Cibernética e Estratégia da sua implementação)

A Política de Segurança Cibernética e Estratégia da sua implementação **(PENSC)** define o enquadramento, os objectivos e as linhas de acção do Estado nesta matéria, de acordo com o interesse nacional.

CAPÍTULO II

Organização de Segurança Cibernética

Artigo 6

(Segurança Cibernética)

A segurança cibernética consiste na protecção dos sistemas de TIC contra danos, roubo ou interrupção dos processos por estes executados e abrange a combinação de pessoas, processos e tecnologia.

Artigo 7

(Estrutura)

A estrutura da Segurança Cibernética é composta pelas seguintes entidades:

a) o Conselho Nacional de Segurança Cibernética;

b) a Autoridade Reguladora do Sector de TIC;

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

d) a Rede Nacional de CSIRTs;

e) os Operadores de Infraestruturas Críticas;

f) os Provedores Intermediários de Serviços;

g) os Operadores de Serviços Essenciais;

h) os Provedores de Serviços Digitais;

i) os Operadores de Centros de Dados;

j) os Operadores de Serviços de Computação em Nuvem.

Secção I

Conselho Nacional de Segurança Cibernética

Artigo 8

(Natureza)

O Conselho Nacional de Segurança Cibernética (CNSC) é o órgão responsável por garantir o alinhamento de políticas, estratégias e outros documentos orientadores da segurança cibernética e, é presidido pelo Ministro que superintende a área de Tecnologias de Informação e Comunicação.

Artigo 9

(Composição e Funcionamento)

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

    a) Representantes dos sectores ou entidades responsáveis pelas áreas de:

        i. Defesa;
        ii. Ordem, Segurança e Tranquilidade Pública;
        iii. Tecnologias de Informação e Comunicação;
        iv. Justiça;
        v. Comunicações;
        vi. Economia e Finanças;
        vii. Educação;
        viii. Saúde;
        ix. Género e Criança;
        x. Energia;
        xi. Transportes;
        xii. Água;
        xiii. Entidade Reguladora de TIC;
        xiv. Entidade Reguladora das Comunicações;
        xv. CSIRT Nacional;
        xvi. Secretariado Técnico.

b) Membros convidados para questões de consulta:

   i. Representante da Academia;

   ii. Representante do Sector Privado; e

   iii. Representante da Sociedade Civil.

c) Outros membros:

   i. Embaixador para Ciber Diplomacia;

   ii. Representante do Ministério Público designado pelo Procurador-Geral da República.

2. Os representantes do sector empresarial, da academia e da sociedade civil no CNSC sao designados pelas respectivas associações confere ao órgão a natureza democrática porque garante a heterogeneidade na governação cibernética.

3. O Presidente da Autoridade Reguladora do Instituto Nacional das Tecnologias de Informação e Comunicação, por sua iniciativa ou a pedido de qualquer dos membros do Conselho, pode convocar outros titulares de órgãos públicos ou convidar outras personalidades de reconhecido mérito para participar em reuniões do Conselho Nacional de Segurança Cibernética.

4. O Conselho de Adminstração do Instituto Nacional das Tecnologias de Informação e Comunicação pode estabelecer os fundamentos técnicos para a criação do Embaixador da Ciber Diplomacia, nos termos a regulamentar.

Artigo 10

(Competências)

1. Compete ao Conselho Nacional de Segurança Cibernética:

a) assegurar a actualização da PENSC;

b) garantir o desenvolvimento das normas e padrões que assegurem um quadro legal de segurança cibernética adequado à realidade nacional;

c) assegurar o desenvolvimento de metodologias, normas e outros instrumentos que assegurem soluções coerentes e uniformes para segurança cibernética;

d) avaliar os riscos da estratégia e propor soluções para a sua eliminação ou mitigação;

e) identificar as Infraestruturas Críticas e acções que visem garantir a sua protecção;

f) avaliar o estágio nacional de segurança cibernética, determinar as necessidades prioritárias e assegurar as respostas apropriadas para cada caso;

g) acompanhar o progresso de implementação da PENSC;

h) coordenar as actividades no âmbito da segurança cibernética;

i) garantir acção conjunta contra crimes cibernéticos;

j) garantir o desenvolvimento e actualização do Observatório Nacional de Segurança Cibernética, cuja informação deve permitir aferir o nível de segurança cibernética do país;

k) garantir a consciencialização das instituições e dos cidadãos em matéria de segurança cibernética, assim como o estabelecimento de mecanismos de prevenção, detecção, monitoria e resolução dos crimes e incidentes de natureza cibernética;

l) propor ao Governo a quem este delegar, a aprovação de decisões de carácter programático relacionadas com a definição e execução da Estratégia Nacional de Segurança Cibernética.

2. O relatório anual de avaliação da execução da Estratégia Nacional de Segurança Cibernética é enviado ao Conselho de Ministros.

Secção II

Autoridade Nacional de Segurança Cibernética

Artigo 11

(Autoridade Nacional)

O Regulador do Sector de TIC é a Autoridade Nacional de Segurança Cibernética.

1. A Autoridade Nacional de Segurança Cibernética é o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC, IP).
2. A Autoridade Nacional de Segurança Cibernética é uma instituição pública, doptada de personalidade jurídica, autonomia administrativa, financeira e patrimonial, assegurando as prerrogativas necessárias ao exercício adequado das suas atribuições.
3. A organização e o funcionamento da Autoridade Nacional de Segurança Cibernética são regulados pelo Estatuto Orgânico aprovado pelo Conselho de Ministros.

Artigo 12

(Competências)

Compete à Autoridade Nacional de Segurança Cibernética, no âmbito da presente Lei:

a) exercer as funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias;

b) garantir que o País use o espaço cibernético de uma forma livre, confiável e segura, através da promoção da melhoria contínua da segurança cibernética

nacional e da cooperação internacional, em articulação com as autoridades competentes;

c) definir e implementar medidas e instrumentos necessários à antecipação, detecção, reacção e recuperação de situações que, face à iminência e ocorrência de incidentes que ponham em causa o interesse nacional, o funcionamento da Administração Pública, os Operadores de Infraestruturas Críticas, os Operadores de Serviços Essenciais e dos Prestadores de Serviços Digitais;

d) garantir a protecção das infraestruturas críticas em coordenação com as entidades reguladores competentes;

e) servir de ponto de contacto único nacional para efeitos de cooperação internacional, sem prejuízo das atribuições legais da entidade que superintende a área da investigação criminal relativas à cooperação internacional em matéria penal;

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

g) emitir pareceres na preparação de qualquer disposição legal de segurança cibernética;

h) actuar em articulação e em estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime, devendo comunicar à autoridade competente, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes;

i) solicitar a quaisquer entidades públicas ou privadas toda a colaboração ou auxílio que julgue necessários para o exercício das suas actividades;

j) estabelecer uma plataforma nacional de partilha de informação e soluções de incidentes de segurança cibernética de uso obrigatório por todos os intervenientes nacionais de ecossistema de segurança cibernética;

k) estabelecer e promover a implementação de programas de consciencialização sobre questões de segurança cibernética, com destaque na protecção da criança e da mulher em actividades no ciberespaço;

l) solicitar o sector público, sector privado, academia e sociedade civil, toda colaboração que se julgue necessária para o exercício das suas actividades;

m) aconselhar e assessorar o sector público, sector privado, academia e sociedade civil em matérias de segurança cibernética;

n) estabelecer e assegurar o cumprimento de códigos de conduta, padrões, normas e promover a adopção de boas práticas e de ética na segurança cibernética;

o) estabelecer padrões e normas para licenciar, registar, acreditar e certificar provedores de produtos e serviços de segurança cibernética;

p) realizar estudos para a identificação de infraestruturas críticas de informação;

q) propor ao Governo a designação e a regulamentação das infraestruturas críticas de informação.

Secção III

Equipa Nacional de Resposta a Incidentes de Segurança Cibernética

Artigo 13

(Natureza)

1. A Equipa Nacional de Resposta a Incidentes de Segurança Cibernética (CSIRT.MZ) exerce a coordenação operacional e estratégica na resposta a incidentes de segurança cibernética em articulação com as equipas de resposta a incidentes de segurança cibernética existentes.

2. A Equipa Nacional de Resposta a Incidentes de Segurança Cibernética funciona na Autoridade Reguladora de Tecnologias de Informação e Comunicação e tem assento no Conselho Nacional de Segurança Cibernética.

Artigo 14

(Competências)

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

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

b) coordenar a Rede Nacional de CSIRTs que é composta por CSIRTs sectoriais, subsectoriais e por CSIRTs institucionais.

c) actuar oficiosamente e quando solicitado por um dos membros da Rede Nacional de CSIRTs, como o centro de coordenação e canalização de informações técnicas e estratégicas servindo de elo de ligação entre a Rede Nacional de CSIRTs e o Conselho Nacional de Segurança Cibernética.

d) servir de elo de ligação entre as redes nacionais de CSIRT e Autoridade Nacional de Segurança Cibernética.

e) criar e manter o Observatório Nacional de Segurança Cibernética;

f) coordenar a resposta a nível nacional de incidentes de segurança cibernética nas instituições públicas, privadas, academia, da sociedade civil em articulação com entidades congéneres a nível internacional sempre que se mostrar necessário.

g) supervisionar as equipes sectoriais de resposta a incidentes de Segurança Cibernética com particular incidência nos sectores das infra-estruturas críticas de informação.

h) garantir a partilha de informação com vista a mitigação de crimes cibernéticos em Moçambique;

i) promover a criação de CSIRTs sectoriais, subsectoriais e institucionais;

j) activar mecanismos de alerta rápido;

k) monitorar os incidentes com implicações a nível nacional;

l) intervir na reacção, análise e mitigação de incidentes;

m) proceder à análise dinâmica dos riscos;

n) assegurar a cooperação com entidades públicas , privadas, academia e sociedade civil;

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

p) participar nos fóruns nacionais de cooperação de equipas de resposta a incidentes de segurança informática;

q) assegurar a representação nacional nos fóruns internacionais de cooperação de equipas de resposta a incidentes de segurança informática;

r) participar em eventos de treino nacionais e internacionais; e

s) criar o Centro de Pesquisa e Análise de Tráfego da Internet (CATI)

2. No exercício das suas funções, o CSIRT Nacional coordena com as entidades ou órgãos reguladores sectoriais competentes, com os CSIRTs sectoriais, com os CSIRTs subsectoriais, com operadores de infraestrutura crítica e Activo de Informação, com outras entidades e órgãos da Administração Pública e privada, instituições da academia, bem como com organizações nacionais e internacionais de natureza semelhante.

Secção IV

Rede Nacional de CSIRTs

Artigo 15

(Natureza)

1. O ecossistema da Rede Nacional de CSIRTs, tem no topo da sua hierarquia o CSIRT Nacional e pressupõe a criação de CSIRTs sectoriais e CSIRTs institucionais.

2. Os sectores do Governo mais apetecíveis a ataques e a crimes cibernéticos têm sido o sector financeiro, comunicações, transportes, saúde, energia e educação, pelo que são encorajados a adoptar medidas arrojadas no combate e resiliência ao cibercrime.

3. 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.

4. Os CSIRTs sectoriais, no âmbito das suas acções de prevenção e combate (resposta) aos abusos no espaço cibernético e ao cibercrime, actuam como elo de ligação entre o CSIRT Nacional e CSIRTs e institucionais.

5. As equipes de resposta a incidentes cibernéticos institucionais devem velar pela segurança cibernética 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

Infraestrutura Crítica Nacional

Artigo 16

(Definição)

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

2. A designação das infraestruturas críticas nacionais é feita sob proposta da Autoridade Reguladora de TIC, após a realização de uma análise de risco desses activos e sistemas de informação, cuja operação é considerada crítica para a disponibilidade e prestação contínua de um serviço essencial no país, nos termos a regulamentar.

3. Cabe à entidade responsável pela gestão ou aos operadores de serviços garantir a aplicação de um conjunto de medidas e técnicas que proporcionam a segurança e protecção dos activos considerados essenciais para o bom funcionamento das infraestruturas.

Artigo 17

(Operadores de Infraestruturas Críticas)

Operador de Infraestrutura Crítica é uma entidade pública ou privada que opera uma infraestrutura crítica.

Secção VI

Provedores Intermediários de Serviços

Artigo 18

(Natureza)

O Provedor Intermediário de Serviço é a pessoa que, em representação de outra pessoa, envia, recebe, ou armazena mensagens de dados, presta serviços de acesso a rede ou serviços a partir dela, nomeadamente:

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

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

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

Secção VII

Operadores de Serviços Essenciais

Artigo 19

(Natureza)

1. O Operador de Serviço Essencial é uma entidade pública ou privada que presta um serviço essencial e enquadram-se num dos tipos de entidades que actuam nos sectores e subsectores constantes do anexo a presente lei e que dele faz parte integrante.

2. Os Prestadores de Serviços Essenciais, devem realizar um registo formal junto a Equipa Nacional de Resposta a Incidentes de Segurança Cibernética, sem prejuízo da privacidade, do âmbito de actuação e das competências que são atribuídas a Autoridade Reguladora de TIC.

Secção VIII

Provedores de Serviços Digitais

Artigo 20

(Natureza)

1. O Provedor de Serviços Digitais é a pessoa colectiva que presta um serviço da sociedade da informação à distância, por via electrónica.

2. Os Provedores de Serviços Digitais prestam os seguintes serviços:

   a) o Serviço de Mercado Online é um serviço digital que permite aos consumidores ou aos comerciantes celebrarem contratos de venda ou de prestação de serviços por via electrónica com comerciantes, quer no sítio na Internet do mercado em linha, quer no sítio na Internet de um comerciante que utilize os serviços de computação disponibilizados pelo mercado em linha;

   b) o Serviço de Motor de Pesquisa Online é um serviço digital que permite aos utilizadores consultarem todos os sítios na Internet, ou sítios na Internet numa determinada língua, com base numa pesquisa sobre qualquer assunto e que fornece ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado;

   c) o Serviço de Computação em Nuvem é um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis.

Artigo 21

(Operadores de Centros de Dados)

1. Cabe aos Operadores e Prestadores de Serviços de Centros de Dados, aplicar um conjunto de medidas e técnicas que proporcionam a segurança e protecção dos dados.

2. Os operadores e prestadores de serviços de Centros de Dados e prestadores de serviço de armazenamento principal devem:

   a) garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos, pelo menos, à mesma protecção e segurança que os dados na rede;

   b) tomar as medidas técnicas e organizativas adequadas à protecção dos dados contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizada ou ilícita.

Artigo 22

(Operadores de Computação em Nuvem)

Os Operadores de Serviços de Computação em Nuvem é a pessoa singular ou colectiva que forneça directa ou indirectamente um conjunto de recursos flexíveis, escaláveis físicos, ou virtuais compartilháveis, além de fornecer e gerir serviços automaticamente mediante solicitação, como um provedor de serviços, intermediário de serviços, agregador de serviços, fornecedor de serviços, revendedor de serviços ou agente fornecedor de serviços.

CAPÍTULO III

Segurança das Redes e dos Sistemas de Informação

Secção I

Segurança de Redes

Artigo 23

(Segurança de Redes de Comunicação de Dados)

As redes do espaço cibernético devem assegurar a integridade, a confidencialidade e privacidade das comunicações mediante a implementação de serviços de segurança lógica e física, estabelecidas no regime jurídico das comunicações electrónicas.

Artigo 24

(Segurança da Internet)

1. A comunicação de dados na rede Internet deve assegurar a integridade, a confidencialidade e 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 25

(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. Para evitar problemas significativos de segurança do Sistema de Nomes de Domínio é proibido o uso de *Emojis* no nome de domínio.

Artigo 26

(Resposta a Incidentes nas Redes do Espaço Cibernético)

1. As redes de comunicações de dados, incluindo a Internet, estão sujeitas as medidas técnicas e operacionais de respostas aos erros, ataques, roubos, acidentes, ciberataques e quaisquer outros incidentes provocados contra si, por via de mecanismos de gestão de respostas de incidentes adequados e eficientes.

2. Os provedores intermediários de serviços e de infraestruturas criticas devem estabelecer os CSIRTs institucionais, que por sua vez são parte de rede nacional de CSIRTs, com mecanismos de coordenação de resposta a incidentes no espaço cibernético definidos na artigo 40 referente aos requisitos de segurança e notificação de incidentes

Secção II

(Medidas de segurança de dados de tráfego e de localização)

Artigo 27

(Segurança de Dados)

1. Os processadores de dados e controladores de dados específicos armazenados numa rede de comunicações electrónicas e sistemas da sociedade da informação, incluindo os dados de tráfego, ficam obrigados a assegurar a confidencialidade e devem ordenar a conservação expedita de dados, sob pena de nulidade.

2. Os dados referidos no número anterior devem ser preservados até 6 (seis) meses.

3. O responsável pelo processamento de dados deve por em prática as medidas técnicas e organizativas adequadas para proteger os dados informáticas contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou ao acesso autorizados, nomeadamente quando o tratamento implicar a sua transmissão para a rede e contra qualquer outra forma de tratamento ilícito.

Artigo 28

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

O provedor intermediário de serviços no espaço cibernético acessível ao público ou prestador de serviços digitais, a quem o armazenamento de dados de tráfego e de localização, relativos à uma determinada comunicação de dados que tenha sido ordenada à conservação, nos termos da legislação específica, deve indicar as outras entidades que nela participem, permitindo a identificação das mesmas.

Artigo 29

(Preservação de provas)

O Provedor Intermediário de Serviços acessíveis ao público ou o Prestador de Serviços Digitais que tenha armazenado num determinado Sistema de Informação, dados de tráfego e de localização necessários a produção de provas, tendo em vista a descoberta da verdade, deve disponibilizar o controlo desses dados ou permitir o acesso ao Sistema de Informação onde os mesmos estejam armazenados, sempre que solicitado pelas autoridades competentes, nos termos da lei.

Artigo 30

(Preservação de dados)

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

2. Os dados referidos no número anterior devem ser conservados por um período de 12 (doze) meses, contados a partir da data da conclusão da comunicação.

Artigo 31

(Dados necessários para identificar a localização do endereço do Protocolo IP)

Para identificar a localização de endereço do protocolo IP, as operadoras de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) a identificação na rede dos endereços físicos dos equipamentos que usaram esse endereço IP;

b) os mapas de endereçamento das redes;

c) os dados que identifiquem a situação geográfica do endereço IP, tomando como referência os registos das Entidades Regionais de Registos da Internet, responsáveis pela distribuição e gestão responsáveis pelos números da Internet, tais como os endereços IP e sistema autónomo de números.

Artigo 32

(Comunicação iniciada ou concluída no território nacional)

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

2. Os dados telefónicos e da Internet relativas a chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados e armazenados pelos Provedores de Serviços de Internet acessíveis ao público, no contexto da oferta de serviços de comunicação.

3. Os dados relativos as chamadas não estabelecidas, não são conservados.

Secção III

Segurança nos Sistemas de Informação

Artigo 33

(Segurança nos Sistema)

O órgão responsável pela promoção da sociedade de informação, os provedores, operadores e prestadores de serviços dos sistemas da sociedade da informação, devem garantir a segurança de qualquer dispositivo ou conjunto de dispositivos que procedem ao armazenamento, tratamento, recuperação ou transmissão de dados informáticos em execução de um programa de computador.

Artigo 34

(Infraestrutura de informática)

Cabe a entidade responsável pela gestão ou aos operadores e prestadores de serviços garantir a aplicação de um conjunto de medidas e técnicas que proporcionam a segurança e protecção dos activos considerados essenciais para bom funcionamento das infraestruturas.

Sessão IV

Programas de Computador e Bases de Dados

Artigo 35

(Programas de computador)

Sem prejuízo do regime jurídico das tecnologias de informação e dos serviços digitais previsto na legislação em vigor, os programas de computador, são aplicáveis as medidas e técnicas da presente Lei.

Artigo 36

(Bases de dados)

Sem prejuízo do disposto no regime jurídico das tecnologias de informação e dos serviços da sociedade da informação, a utilização das bases de dados deve obedecer as regras técnicas e procedimentos especializados de protecção adequada acesso, armazenamento, duplicação de arquivos, tratamento e recuperação de informação automatizada.

CAPÍTULO IV

Requisitos de Segurança e Notificação de Incidentes

Artigo 37

(Incidentes de segurança cibernética de impacto significativo)

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

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

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

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

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

Artigo 38

(Definição de 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 da legislação específica.

Artigo 39

(Definição de 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 Infraestruturas Críticas;
   d) Provedores Intermediários de Serviços;
   e) Operadores de Serviços Essenciais;
   f) Provedores de Serviços Digitais;
   g) Operadores de Centros de Dados;
   h) Operadores de Plataformas de Computação em Nuvem;
   i) quaisquer outras entidades que utilizem redes e sistemas de informação.

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

3. Os requisitos de notificação de incidentes não se aplicam:
   a) às redes e sistemas de informação directamente relacionados com o comando e controlo das 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 40

(Requisitos de segurança para a Administração Pública e Operadores de Infraestruturas Críticas)

1. A Administração Pública e os Operadores de Infraestruturas 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. A Administração Pública e os Operadores de Infraestruturas 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 41

(Notificação de incidentes para a Administração Pública e Operadores de Infraestruturas Críticas)

1. A Administração Pública e os Operadores de Infraestruturas Críticas devem estabelecer CSIRTs institucionais e notificar ao respectivo CSIRT sectorial e ao CSIRT Nacional os incidentes com um impacto relevante na segurança das redes e dos sistemas de informação, no prazo definido na legislação específica.

2. A notificação dos Operadores de Infraestruturas Críticas inclui informação que permita ao CSIRT Nacional 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, a Autoridade Nacional de Segurança Cibernética presta ao notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente, informações que possam contribuir para o tratamento eficaz do incidente.

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

7. A Administração Pública e os Operadores de Infraestruturas Críticas são obrigados a submeter ao CSIRT sectorial e para o CSIRT Nacional 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 42

(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 43

(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 CSIRT Nacional os incidentes com um impacto relevante na continuidade dos serviços essenciais por si prestados, no prazo definido na legislação específica.

2. A notificação inclui informação que permita à Autoridade Nacional de Segurança Cibernética 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) o duração do incidente;

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

5. Com base na informação prestada na notificação, a Autoridade Nacional de Segurança Cibernética 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, a Autoridade Nacional de Segurança Cibernética 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, a Autoridade Nacional de Segurança Cibernética 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. A Autoridade Nacional de Segurança Cibernética transmite as notificações referidas no n.º 1 do presente artigo, aos pontos de contacto únicos dos outros Estados afectados.

9. A Autoridade Nacional de Segurança Cibernética, 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 CSIRT Nacional 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 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 44

(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. O presente artigo não se aplica às microempresas e às pequenas empresas.
5. Os elementos constantes dos números 1 a 3 do presente artigo são objecto de regulamento específico.

Artigo 44

(Notificação de incidentes para os Prestadores de Serviços Digitais)

1. Os Prestadores de Serviços Digitais notificam o Autoridade Nacional de Segurança Cibernética dos incidentes com impacto substancial na prestação dos serviços digitais, no prazo definido na legislação específica.
2. A notificação referida no número anterior inclui informação que permita à Autoridade Nacional de Segurança Cibernética determinar a importância dos impactos transfronteiriços.
3. A notificação não acarreta responsabilidades acrescidas para a parte notificante.
4. A fim de determinar se o impacto de um incidente é substancial, são tidos em conta os seguintes parâmetros:
    a) o número de utilizadores afectados pelo incidente, em particular os utilizadores que dependem do serviço para prestarem os seus próprios serviços;
    b) a duração do incidente;
    c) a distribuição geográfica, no que se refere à zona afectada pelo incidente;
    d) o nível de gravidade da perturbação do funcionamento do serviço;

e) 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 a que se refere o n.º 2 do artigo anterior.

6. Se os incidentes referidos no n.º 1 dizem respeito a dois ou mais Estados, a Autoridade Nacional de Segurança Cibernética informa os pontos de contacto únicos dos outros Estados afectados.

7. No caso referido no número anterior, a Autoridade Nacional de Segurança Cibernética salvaguarda a segurança e os interesses do prestador de serviços digitais.

8. A Autoridade Nacional de Segurança Cibernética, 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 CSIRT Nacional 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 45

(Requisitos de segurança para Operadores de Centros de Dados)

1. Um operador de Centro de Dados é uma entidade dedicada ao arranjo, processamento, armazenamento e distribuição de dados. As empresas e outras organizações utilizam esses centros de dados para melhorar a produção e a lucratividade de seus negócios.

2. 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.

3. Os Operadores de Centros de Dados devem ser licenciados pela Autoridade Reguladora de TIC.

Artigo 46

(Notificação de incidentes para Operadores de Centros de Dados)

1. Os Operadores de Centros de Dados devem notificar seus assinantes, antepadamente 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 CSIRT Nacional antepadamente de qualquer incidente de segurança cibernética 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. 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 Nuvem são obrigados a submeter ao CSIRT sectorial e para o CSIRT Nacional 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 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 47

(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 nos termos da legislação específica.

Artigo 48

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

1. O Provedor de Serviços de Computação em Nuvem deve notificar aos seus assinantes, sem atraso injustificado de quaisquer incidentes de segurança cibernética, incluindo

vazamento de dados e o que afecta ou pode afectar o conteúdo do assinante, dados ou quaisquer serviços fornecidos a esses assinantes.

2. O Provedor de Serviços de Computação em Nuvem deve notificar ao CSIRT Nacional de imediato de qualquer incidente de segurança cibernética 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 CSIRT Nacional 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 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 49

(Notificação voluntária de incidentes)

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

2. No tratamento das notificações voluntárias, aplica-se o disposto no artigo 17.º, com as necessárias adaptações.

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

CAPÍTULO V

Respostas à Ameaças e Incidentes de Segurança Cibernética

Artigo 50

(Acções para prevenir e gerir incidentes de segurança cibernética)

Quando o CSIRT Nacional tiver recebido informações sobre uma ameaça ou incidente de segurança cibernética de alto impacto significativo, deve informar a entidade ou órgão regulador sectorial competente ou ao CSIRT Sectorial correspondente, ou, na falta deste, à Autoridade Reguladora de TIC, 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 segurança cibernética em uma infraestrutura crítica, buscando:

a) avaliar o impacto ou potencial impacto da ameaça ou incidente;

b) eliminar a ameaça de segurança cibernética ou prevenir qualquer dano ou dano adicional resultante do incidente de segurança cibernética;

c) impedir que um novo incidente de segurança cibernética surja dessa ameaça ou do incidente de segurança cibernética.

Artigo 51

(Responsabilidade pela notificação de incidente de segurança cibernética)

Caso as informações sobre um incidente de segurança cibernética de impacto significativo sejam inicialmente recebidas por um CSIRT Sectorial, ele será responsável por notificar ao CSIRT Nacional, para que possa ser correlacionado com outros incidentes significativos reportados de outros Sectores de Infraestrutura Crítica.

Artigo 52

(Meios de prevenção e gestão de incidentes)

As acções mencionadas no artigo 32 permitem que o CSIRT Nacional ou CSIRT Sectorial, se houver, tome as seguintes medidas para proteger a segurança cibernética da Infraestrutura Crítica:

1. Exigir ao Operador de Infraestrutura Crítica informe sobre qualquer incidente de segurança cibernética de alto impacto significativo pelo qual é afectado;

2. Exigir ao Operador de Infraestrutura 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;

3. Solicitar ao Operador de um Sistema de Informação ligado ao Operador de uma Infraestrutura Crítica que realize qualquer acção dentro da estrutura para ajudar na gestão de incidentes de segurança cibernética:
    a) preservar o estado do sistema de informação;
    b) monitorar o sistema de informação por um período de tempo específico;
    c) realizar uma análise do sistema de informação para detectar vulnerabilidades de segurança cibernética, avaliar a maneira e a extensão do sistema de informação afectado pelo incidente de segurança cibernética.

Artigo 53

(Entrega de informações)

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

2. As informações que são entregues ao CSIRT Sectorial, CSIRT Nacional e a Autoridade Reguladora do Sector de TIC, são considerados reservados e confidenciais.

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

Artigo 54

(Divulgação Responsável de Vulnerabilidades)

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

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

a) se não tiver sido feita sob coacção ou ameaça de publicação de informações e não ~~foi~~ tiver sido solicitada a recompensa;

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

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

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

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

Artigo 55

(Identificação de Operadores de Serviços Essenciais)

As entidades do sector das infraestruturas digitais devem comunicar de imediato a Autoridade Reguladora do Sector de TIC e ao CSIRT Nacional o exercício da respectiva actividade.

Artigo 56

(Identificação de Prestadores de Serviços Digitais)

1. Os Prestadores de Serviços Digitais devem comunicar de imediato a Autoridade Reguladora do Sector de TIC e ao CSIRT Nacional o exercício da respectiva actividade.

2. O dever de notificação referido no número anterior não é aplicável às micro e às pequenas empresas, tal como definidas em legislação específica.

CAPÍTULO VI

Disposições finais

Artigo 57

(Contravenções)

1. A violação das disposições da presente Lei e demais legislação aplicável ao sector das Tecnologias de Informação e Comunicação, que não são caracterizadas por lei como crime, constitui contravenção punível com multa ou sanção estabelecidas em legislação específica.

2. Constituem contravenções todos os factos ilícitos que preencham um tipo legal correspondente á violação de disposições legais relactivas a segurança cibernética para as quais caiba multa, suspensão de licenças, certificados, autorizações ou proibição de operação.

Artigo 58

(Multas)

O Valor da multa aplicável pela violação das normas previstas na presente Lei, é fixada nos termos a regulamentar.

Artigo 59

(Crimes)

Os crimes contra a segurança cibernética são previstos e punidos de acordo com a legislação especifica, aplicando-se subsidiariamente a legislação penal geral.

Artigo 60

(Receitas)

As receitas revertem-se em:

a) 20 % para o Estado;

b) 80 % para à Entidade Reguladora.

Artigo 61

(Regime subsidiário)

É aplicável subsidiariamente a presente Lei, em tudo que se refira à matéria da segurança cibernética o regime jurídico aplicável as Tecnologias de Informação e Comunicação.

Artigo 62

(Regulamentação)

Compete ao Governo Regulamentar a presente Lei no prazo de 180 dias a contar da data da sua publicação no Boletim da República.

Artigo 63

(Entrada em vigor)

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

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

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

Promulgada aos …de Fevereiro de 2023

Publique se.

O Presidente da Republica, Filipe Jacinto Nyusi

ANEXO I

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

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

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

ANEXO II

Glossário

Para efeitos do presente regulamento, entende-se por:

A

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

Ameaça ¬ é a actividade, conhecida ou suspeita, que, se ocorrer, teria ou poderia ter um efeito adverso na segurança cibernética de um ou infra-estrutura mais crítica ou qualquer um de seus componentes, incluindo sistemas informáticos complementares ou acessórios.

Ameaças Cibernéticas ¬ é o sequestro

C

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

E

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

Equipa de resposta a incidentes de segurança cibernética ¬ a equipa que actua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação;

Especificação técnica ¬ um documento que define os requisitos técnicos que um produto, processo, serviço ou sistema devem cumprir;

Evento ¬ qualquer ocorrência observável em um sistema, rede ou activo tecnológico;

I

Incidente ¬ qualquer evento que tenha ou possa ter iminentemente um efeito adverso na Segurança Cibernética de uma ou mais infraestruturas crítica, de qualquer um de seus

componentes, da informação processada, armazenado ou transmitido por ele, ou que constitua uma infracção ou ameaça iminente de violação das políticas ou procedimentos da empresa políticas actuais de segurança cibernética ou uso aceitável;

Incidente ¬ um evento com um efeito adverso real na segurança das redes e dos sistemas de informação;

Indicadores de comprometimento ¬ são todas as informações relevantes que descrevem qualquer incidente de segurança cibernética, evento, actividade maliciosa e/ou artefacto, analisando seus padrões comportamental;

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

N

Norma ¬ uma especificação técnica, aprovada por um organismo de normalização reconhecido, para aplicação repetida ou continuada, cuja observância não é obrigatória;

O

Operador ¬ é a entidade ou órgão responsável pela operação de uma infraestrutura crítica. Nos casos em que a infraestrutura crítica é propriedade conjunta de mais de uma pessoa ou operado por mais de uma entidade, inclui cada operador individualmente ou em conjunto. Quando uma infra-estrutura crítica é propriedade do Governo e for explorada por qualquer entidade pública, privada ou de qualquer outro tipo, será tratada como operadora da infraestrutura crítica para efeitos da presente lei.

Operador de infraestrutura crítica ¬ uma entidade pública ou privada que opera uma infraestrutura crítica;

Operador de serviços essenciais ¬ uma entidade pública ou privada que presta um serviço essencial;

P

Ponto de troca de tráfego ¬ uma estrutura de rede que permite a interligação de mais de dois sistemas autónomos independentes a fim de facilitar a troca de tráfego na *Internet;*

Prestador de serviços digitais ¬ uma pessoa colectiva que presta um serviço digital;

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

R

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

Registo de nomes de domínio de topo ¬ uma entidade que administra e opera o registo de nomes de domínio da *Internet* de um domínio de topo específico;

Representante do prestador de serviços digitais ¬ uma pessoa singular ou colectiva, estabelecida em (União Europeia,) MOCAMBIQUE expressamente designada para actuar por conta de um prestador de serviços digitais aí não estabelecido;

Risco ¬ uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação;

S

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

Serviço de computação em nuvem ¬ um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis;

Serviço de mercado em linha ¬ um serviço digital que permite aos consumidores ou aos comerciantes celebrarem contractos de venda ou de prestação de serviços por via electrónica com comerciantes, quer no sítio na *Internet* do mercado em linha, quer no sítio na *Internet* de um comerciante que utilize os serviços de computação disponibilizados pelo mercado em linha;

Serviço de motor de pesquisa em linha ¬ um serviço digital que permite aos utilizadores consultarem todos os sítios na *Internet*, ou sítios na *Internet* numa determinada língua, com base numa pesquisa sobre qualquer assunto e que fornece ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado;

Serviço digital ¬ um serviço da sociedade da informação prestado à distância, por via electrónica;

Serviço essencial ¬ é qualquer serviço que se revele necessário para a segurança nacional, defesa, relações exteriores, economia, saúde, segurança ou ordem pública da República Dominicana.

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

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

Sistema de informação ¬ é todo o dispositivo ou conjunto de dispositivos que usam tecnologias de informação e comunicação, bem como qualquer sistema de alta tecnologia e tecnologias emergentes, incluindo sistemas electrónicos, de computador, telemáticos e de comunicação. telecomunicações que, isolada ou conjuntamente, servem para gerar, enviar, receber, arquivar ou processar informações, documentos digitais, mensagens de dados, entre outros. Refere-se a qualquer sistema de tecnologia da informação ou qualquer sistema de tecnologia operacional como um sistema de controle industrial, um controlador lógico programável, um controle supervisor e sistema de aquisição de dados, ou um sistema controle distribuído.

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

T

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

V

Vinculação com um operador de infraestrutura crítica ¬ refere-se a ao fato de uma pessoa ser funcionário, funcionário ou fornecedor de um operador de uma infraestrutura crítica. No caso dos sistemas de informação, esta vinculação refere-se ao fato de que estes são de propriedade ou administrados por funcionários e funcionários do operador de uma infraestrutura crítica ou que são usados para fornecer um serviço a ele.

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